Compass Learning Centre

E-Safety & ICT Policy 2021-2022

Governors' Committee responsible	Full Governing Body
Link Governor	Chair of Governors
Link SLT	School Business Manager
Date Reviewed	July 2021
Next Review Date	July 2022
Key Linked Policies / Documents	Child Protection / Safeguarding Policies Anti-Bullying Policy Data Protection Policy Learning & Teaching Policy Staff Code of Conduct See also pages 91 – 97.

Our aim is to help all our learners unlock their potential in life and work

Signed Signed

Chair of Compass Governing Board Head teacher

Equality Impact Assessment – initial screening record

• What area of work is being considered?	E-Safety & ICT Policy
• Upon whom will this impact?	Staff, Students, Parents / Carers

• How would the work impact upon groups, are they included and considered?

The Equality Strands	Negative Impact	Positive Impact	No impact
Minority ethnic groups		√	
Gender		√	
Disability		√	
Religion, Faith or Belief		√	
Sexual Orientation		√	
Transgender		√	
Age		√	
Rurality		√	

• Does data inform this work, research and/or consultation. And has it been broken down by the equality strands?

The Equality Strands	No	Yes	Uncertain
Minority ethnic groups	√		
Gender	√		
Disability	√		
Religion, Faith or Belief	√		
Sexual Orientation	√		
Transgender	√		
Age	√		
Rurality	√		

• Does the initial screening highlight potential issues that may be illegal? **No**

Further comments:-

Initial screening carried out by School Support Manager
Signed: Kerry Taylor Dated: July 2021

Comment by Headteacher:
Alison Glazier

Contents

Introduction

SWGfL / UK Safer Internet Centre

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety.

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk. SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa. More information about its wide ranging online safety services for schools can be found on the SWGfL website – swgfl.org.uk

360 degree safe Online Safety Self Review Tool

360 degree safe is an online, interactive Self Review Tool which allows schools / academies to review their online safety policy and practice. It is available, free of charge, to all schools / academies - with over 10,000 registrations, since its introduction in 2009. There are also specific versions of the tool available for Wales and Scotland. You can register at 360safe.org.uk.

Schools / academies choose one of 5 level statements in each of the 28 aspects. The tool provides an "improvement action" describing how the school / academy might move from that level to the next. Users can immediately compare their levels to the benchmark levels of all the schools / academies using the tool. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources / good practice guidance and collates the school's action plan for improvement. Sections of these policy templates can also be found in the links / resources section in 360 degree safe.

Schools that reach required benchmark levels can apply for assessment for the Online Safety Mark, involving a half day visit from an accredited assessor who validates the school's self-review. More information about the Online Safety Mark can be found at: https://360safe.org.uk/Accreditation/OnlineSafetyMark

Online Safety BOOST and BOOST+ – Schools Online Safety Toolkit

Online Safety BOOST and BOOST+ packages bring you extra empowerment and support to deal with your online safety challenges, official or otherwise. It comprises a toolkit of apps, services, tools and resources that all go to save time, equip your school to be more sensitive to, and better manage, online safety situations and issues. This document will reference specific aspects of BOOST to illustrate how it integrates with policy. For further information on BOOST, or to subscribe, please visit https://boost.swgfl.org.uk/

Online Data Protection Self-Review Tool

360data is a unique self-review tool designed to help organisations test and improve their data protection policies and practices. Built on the same approach as the award-winning 360 Degree Safe, this tool will help your organisation understand what systems are currently in place and how to improve these.

During your review, you will be able to generate reports with a list of improvement actions to help you move forward with your organisation's data security. All the resources required to enact those recommendations is included in the tool.

The Online Safety Template Policies

These School / Academy Online Safety Template Policies are intended to help school / academy leaders produce a suitable Online Safety policy document which will consider all current and relevant issues, in a whole school / academy context, linking with other relevant policies, such as the Child Protection / Safeguarding, Behaviour and Anti-Bullying policies.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools / academies are bound. Schools / academies must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school / academy. The policy will also form part of the school's / academy's protection from legal challenge, relating to the use of digital technologies.

In England, schools / academies are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. From 2015 there are additional duties under the Counter Terrorism and Securities Act 2015 which require schools / academies to ensure that children are safe from terrorist and extremist material on the internet. Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

These template policies suggest policy statements which, in the view of SWGfL, would be essential in any school / academy Online Safety Policy, based on good practice. In addition there are a range of alternative statements that schools / academies should consider and choose those that are most suitable, given their particular circumstances.

An effective School / Academy Online Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school / academy community.

It is suggested that consultation in the production of this policy should involve:

- Governors / Directors
- Teaching Staff and Support Staff
- Students / pupils
- Parents
- Community users and any other relevant groups.

Due to the ever changing nature of digital technologies, it is best practice that the school / academy reviews the Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Given the range of optional statements offered and the guidance notes provided, this template document is longer than the resulting school policy is likely to be. It is intended that, while covering a complicated and ever-changing aspect of the work of the school / academy, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

The template uses a number of alternative terms e.g. Headteacher / Principal; Governors / Directors; students / pupils; local authority / other responsible body. Schools / Academies will need to choose which term is relevant and delete the other accordingly.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that schools / academies would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD, it is suggested that these should be an essential part of a school / academy Online Safety Policy.

The first part of this document (approximately 25 pages) provides a template for an overall Online Safety Policy for the school / academy. The appendices contain more detailed and more specific policy templates and agreement forms. It will be for schools / academies to decide which of these documents they chose to amend and adopt.

Compass Learning Centre

Online Safety Policy

July 2021

SWGfL Education that Clicks

UK Safer Internet Centre

360 safe the online safety self-review tool

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of: /

- Headteacher / Senior Leaders
- DSL Kerry Taylor
- Online Safety Officer / Coordinator
- Additional staff on E-safety Committee
- Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings, reviews of incidents and e-safety practises to be done on termly basis

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	*15 July 2021*
The implementation of this Online Safety policy will be monitored by the:	*– Online Safety Coordinator and DSL*
Monitoring will take place at regular intervals:	*Termly*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*at least once a year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*June 2021*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police,*

The school will monitor the impact of the policy using: *(delete / add as relevant)*

- Logs of reported incidents and records on MyConcern
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

This policy applies to all members of the Compass Learning Centre (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers the Head teacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the Compass Learning Centre but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Compass Learning Centre will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Compass Learning Centre.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*. The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Officer*.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section.
- *The Headteacher /Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Keeping up to date with Boost Online Safety training.*
- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Officer.*

Online Safety Officer

- leads the Online Safety Group meeting on a termly basis.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Recommends training and advice for staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The Network Manager / Technical Staff Computing is responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack.

- that the *school* meets required online safety technical requirements and any *Local Authority / other relevant body* Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- *the filtering applied is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.*
- *that monitoring software / systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Online Safety Officer for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems and recorded.
- online safety issues are embedded in all aspects of the curriculum and other activities, to aid pupils understanding and follow the Online Safety Policy and acceptable use policies and ensure they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the Compass learning centre community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Officer (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety Policy / documents. .
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

The online safety group consists of a range of school staff, this includes a senior leader, teacher, teaching support and admin support staff

Students / Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *Compass Learning Centre's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the all devices connected to e-safety in an appropriate way. The *Compass Learning Centre* will take every opportunity to

help parents understand these issues through *parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- *their children's agreement to hand in their personal devices at the beginning of day at the school*

Community Users

Community Users who access school systems/ website / Learning Platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of tutorial / pastoral activities and should be displayed around centre.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need to adhere to acceptable use agreements adopt safe and responsible use both within and outside school / academy.

- Staff should act as good role models in their use of digital technologies by adhering to Staff acceptable use policy.
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. swgfl.org.uk www.thinkuknow.com www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)*

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community*

Education & Training

Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly using Online Safety BOOST (https://boost.swgfl.org.uk/) or similar
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Officer (or other nominated person) will provide advice / guidance to individuals as required.

Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents.
- Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the Compass Learning Centre network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager. Users are responsible for the security of their username and password.
- Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. There is a clear process in place to deal with requests for filtering changes. Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices will be school owned/provided and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of the provided devices in a school context is educational. The use of mobile technologies should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies

The Compass Learning Centre allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*no*	*no*	*no*
Internet only						*Yes for meeting purposes*
No network access					*yes*	*Yes*

School owned / provided devices:

- Are allocated based on the needs of the staff member related to their role
- Are to be used predominately in school but can be taken offsite, it is the responsibility of the user to keep the device safe and use in line with the Acceptable use Agreement
- Technical support can be sought from Schoolcare
- All students and staff have access to Office 365 which allows the use of Microsoft applications and cloud storage

Personal devices:

Staff may bring their own mobile into school but must only access this before and after school and at break or lunchtimes when not on duty. All personal mobile technology is not to be used for school business.

- Visitors may use their own devices when taking part in a meeting/conference where information is required from another agency/service
- No technical support is available for personal mobile devices
- Filtering of the internet connection to these devices
- Data Protection

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- The school has the right to take, examine and search users devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press I
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school / academy policies concerning the sharing, distribution and publication of those images. Those images only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website will not include anything which identifies the pupils.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Written with consideration for the data protection arrangements for the UK General Data Protection Regulation (GDPR).

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults					Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed		Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought into the school	x								x
Use of mobile phones in lessons				x					x
Use of mobile phones in social time (breaks)	x								x
Taking photos on mobile phones / cameras				x*					x
Use of other mobile devices e.g. tablets, gaming devices				X*					x
Use of personal email addresses in school, or on school network				x					x
Use of school email for personal emails				x					x
Use of messaging apps				x					x
Use of social media				x					x
Use of blogs				x					x

*unless using school camera, ipad or gaming device for educational purpose

When using communication technologies Compass Learning Centre considers the following as good practice:

- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and students / pupils should therefore use*

only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. (Online Safety BOOST includes an anonymous reporting app Whisper – https://boost.swgfl.org.uk/)
- Any digital communication between staff and students / pupils or parents / carers via email must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority / MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Online Safety BOOST includes unlimited webinar training on this subject: https://boost.swgfl.org.uk/)
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- **be aware that Compass Learning Centre does not permit staff to use their personal social media during the working day, and use may result in disciplinary action;**

School social media accounts

The school does not permit access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school/academy in online media (newspaper or social media for example) https://boost.swgfl.org.uk/)

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce				x	
File sharing			X*		
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting e.g. Youtube			X**		

*OneDrive should be used for this and should be only for academic and professional purposes not personal.

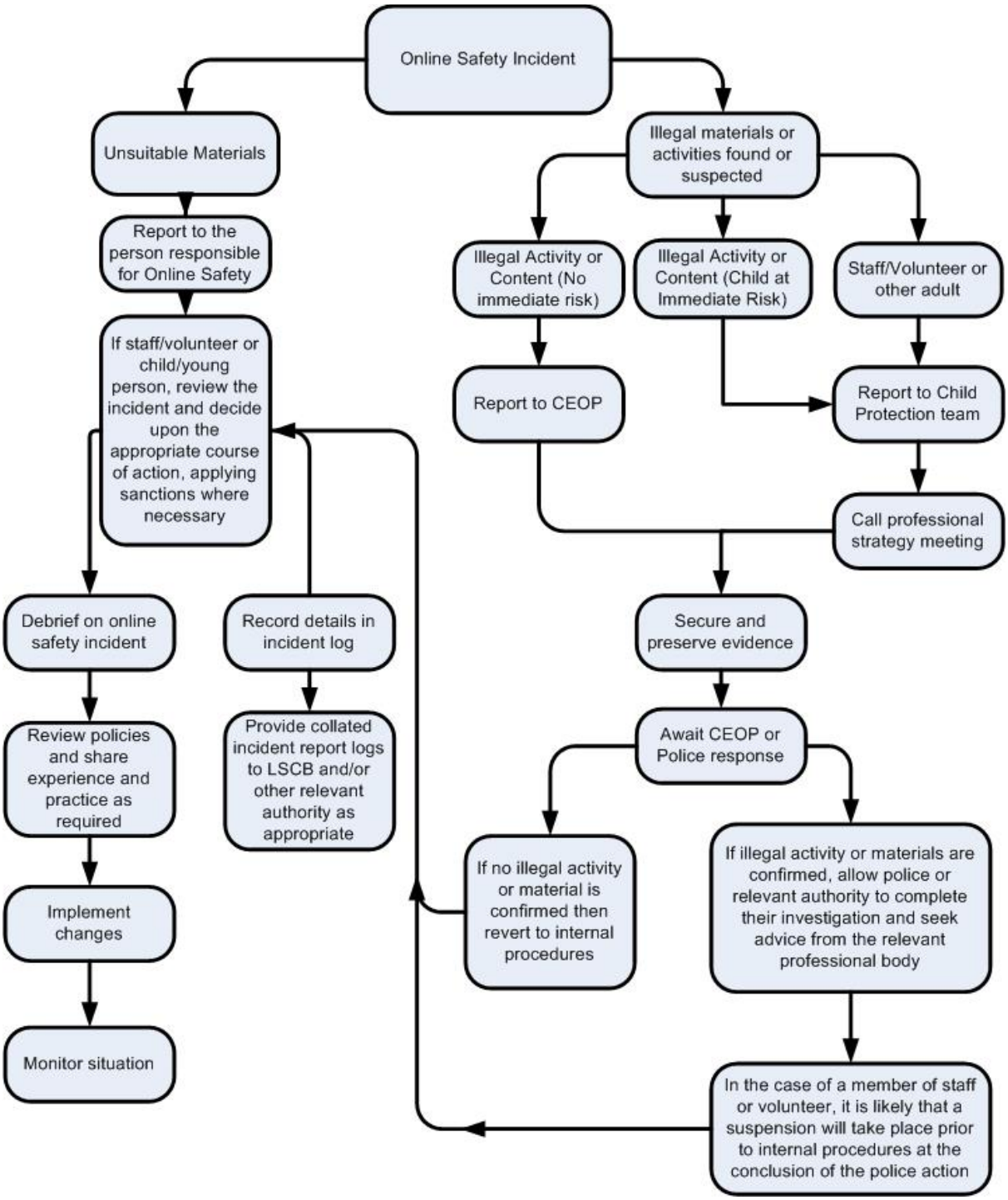
**Only to be used for educational purposes by staff assigned a staffproxy for use on their account. All videos must be checked content is appropriate prior to sharing.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School / Academy Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows.

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X		x	X		
Unauthorised use of non-educational sites during lessons	X				x			X	x
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	x				x		X	X

Unauthorised / inappropriate use of social media / messaging apps / personal email	X	x			x		x		x
Unauthorised downloading or uploading of files	X	x			x	x	x		x
Allowing others to access school network by sharing username and passwords	X	x	X		x	x	x		x
Attempting to access or accessing the school network, using another pupil's account	X	x	X		x	x	x		X
Attempting to access or accessing the school network, using the account of a member of staff	X	x	X		x	x	x		X
Corrupting or destroying the data of other users	X	x	x		x	X	x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	x	x	x		x		X	
Continued infringements of the above, following previous warnings or sanctions	X			x	x	x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	x	x		x	x	x	x	x
Using proxy sites or other means to subvert the school's filtering system	X	x			x	x	x		X
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x	x	X	
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x	x	x	x		X

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			x	x
Inappropriate personal use of the internet / social media / personal email	x				x	x		
Unauthorised downloading or uploading of files	x	X	x		x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	x	x		x	x	x	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x		x	X		x
Deliberate actions to breach data protection or network security rules	x	X	x	x	x	x	x	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x	x	x	x	x	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x		x	x	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x	x	x	x	x	x	x	X
Actions which could compromise the staff member's professional standing	x	x	x	x	x	x	x	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x		x		x	X

Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x		x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	X		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x	x	x		x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x	x

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

SWGfL Online Safety Policy Templates

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendices

Pupil Acceptable Use Agreement

School Policy

Digital technologies have become an important part of everyday lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people off-line that I have communicated with on-line and inform a trusted adult if someone asks me to meet them.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).
- I understand that if I need to loan equipment from Compass Learning Centre my parent/carer and I need to complete the Equipment Loan and User agreements.
- I understand that the devices belong to Compass Learning Centre and are loaned to me.
- I understand that I need to follow the Pupil Acceptable Use policy for all loaned equipment.
- I understand that my parent/carer and I will have to pay for the repair or replacement of any item lost, stolen or damaged whilst on loan to me

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and benefits of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones / USB devices etc) in school. I will hand these devices in at the beginning of each day to be securely stored and collect at the end of each day. I understand that, if I do use my own devices in the school there will be sanctions for this.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened. I understand that all devices used in school or loaned to me by the school, belong to the school. The school may make a charge to my parent/carer for any damage caused to any devices loaned to me, amounting to the cost of repair or replacement of the device.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use specified sites with permission.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices
- Use of my own devices in the school e.g. mobile phones, gaming devices USB devices, cameras etc. is not authorised. If personal devices are brought in -hand ins must take place at start of school day, for devices to be securely stored and returned at end of the day
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature:

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupils Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care and the expectation on parent/carers should damage occur to a device loaned to the pupil. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: .....

Student / Pupil Name:..... .....

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....

Date: .....

Use of Digital / Video Images

The use of digital / video images plays an important part in some learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent / Carers Name:..... Student / Pupil Name:.....

As the parent / carer of the above student / pupil, I agree to the school taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
• to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Images may be used as evidence to support qualifications, use on internal display boards	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

The school uses *Office 365* for *students* and staff. This permission form describes the tools and pupil / student responsibilities for using these services. The following services are available to each *student* as part of the school's online presence in *Office 365*.

Using *Office 365* will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Student / Pupil Name: ..... Parent / Carers Name:.....

Signed: ..... Date: .....

Device loan agreement for Student

1. This agreement is between:

1) The Compass Centre

2) Name of parent _____ Name of Student _____

And governs the use and care of devices assigned to the parent's child. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the student _____ for the purpose of school work

2. This agreement sets the conditions for taking a _____ home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

If you're providing devices to pupils who are eligible for the pupil premium insert:
If the equipment is damaged, lost or stolen, contact the school office on 01305 206530.
I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy if the pupil engages in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact the school office on 01305 206530 or on the email office@compass.dorset.sch.uk

6. Return date

I will return the device in its original condition to the school office within 14 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form or by typing my name and my child's name I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	

PUPIL'S FULL NAME	
PARENT'S FULL NAME	

Equipment loan form for pupils

To be filled out by staff signing out the equipment.

DETAILS OF PUPIL	
NAME	
CLASS	
YEAR GROUP	
ADDRESS	
PARENT'S TELEPHONE NUMBER	
PARENT'S EMAIL	
LOAN DETAILS	
LOAN DATE	
DATE RETURNED	
EQUIPMENT DETAILS	
TYPE	
MAKE	
MODEL	
SERIAL NUMBER	
ASSET NUMBER	
EQUIPMENT CONDITION	

ACCESSORY DETAILS	
DESCRIPTION	QUANTITY

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from

the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to take or record record these images. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites, gambling, gaming or shopping sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will record all communications on relevant systems e.g SIMS
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- When I use the school desktop computers, mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement. I will not use my own mobile devices during school time and will adhere to the rules set by the school about such use..
- I will not use personal email addresses on the school ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings..
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened. Damage or theft of mobile devices loaned to me by the school are my responsibility to look after and

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Device loan agreement for staff

1. This agreement is between:

1) The Compass Centre

2) Staff member

.....

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the employee .....

2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform my line manger and I acknowledge that I may be responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on staff code of conduct.

4. Personal use

I will only use this device for personal use and will not loan the equipment to any other person provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined above

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure the equipment locks if left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact Schoolcare on the email helpdesk@c-c-c.co.uk

6. Return date

I will return the device in its original condition to the school office within 14 days of being requested to do so. .

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

7. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME	
SIGNATURE	

Equipment loan form for staff

To be filled out by staff signing out the equipment.

DETAILS OF LOANEE	
NAME OF STAFF MEMBER	
ADDRESS	
TELEPHONE NUMBER	
EMAIL	
LOAN DETAILS	
LOAN DATE	
DATE RETURNED	
EQUIPMENT DETAILS	
TYPE	
MAKE	
MODEL	
SERIAL NUMBER	
ASSET NUMBER	
EQUIPMENT CONDITION	
ACCESSORY DETAILS	

DESCRIPTION	QUANTITY

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are

published it will not be possible to identify by name, or other personal information, those who are featured.

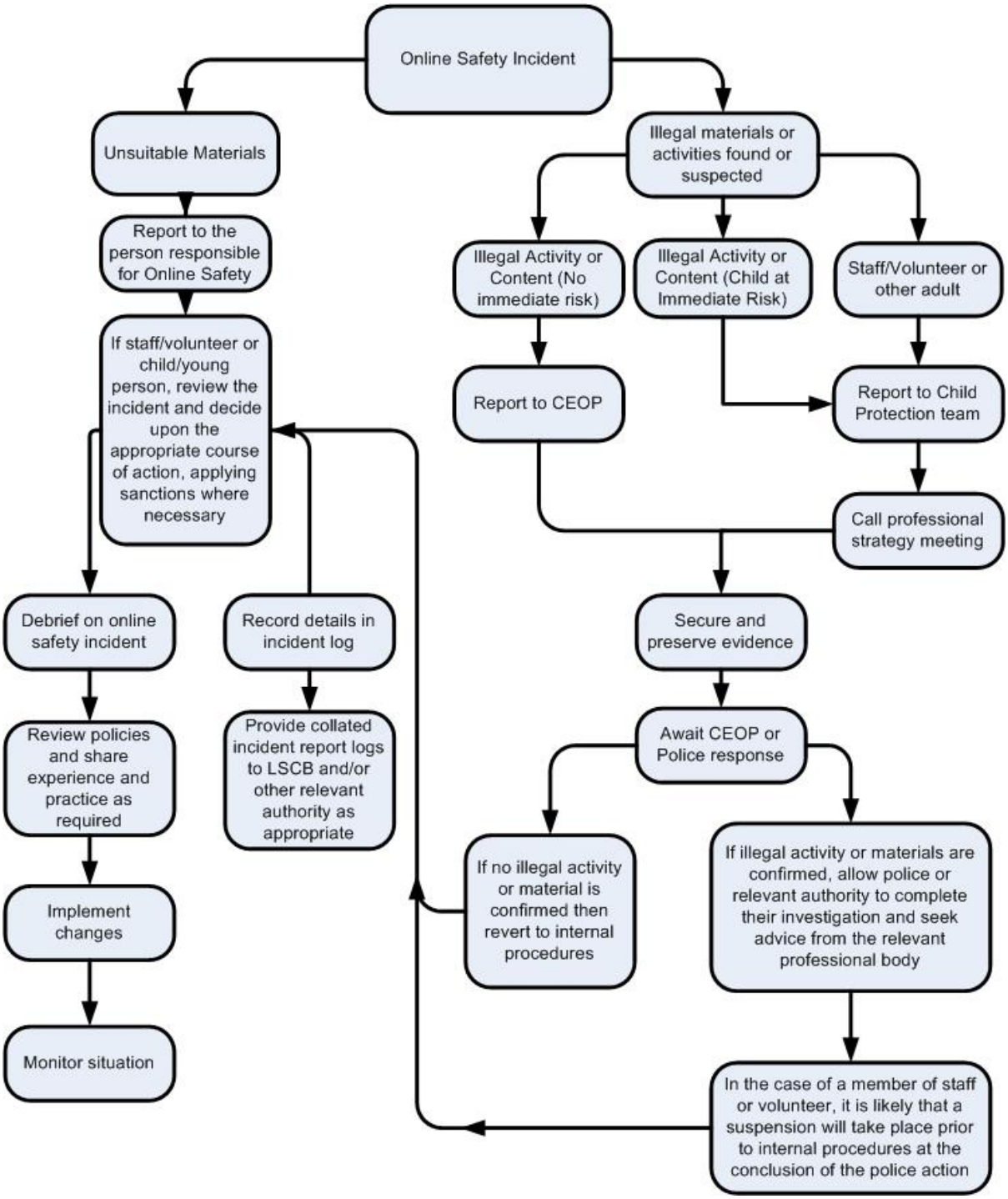
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ..... Signed: .....

Date: .....

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Schoolcare.

Technical Security

Policy statements

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems.

- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Schoolcare is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place the school office for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).
- An agreed policy is in the school office for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by Schoolcare. Any changes carried out must be notified to the manager of the password security policy.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below

Staff Passwords

- All staff users will be provided with a username and password (changeable on first login) by the school business manager or HR Administrator who will keep an up to date record of users and their usernames.

- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- should be changed at least every 60 to 90 days
- should not be re-used for 6 months and be significantly different from previous passwords created by the same user.

Pupil Passwords

- All users will be provided with a username and password by school business manager who will keep an up to date record of users and their usernames.
- Students / pupils will be taught the importance of password security
- School password routines should model good password practice for users
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons during ICT safety lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The school business manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the person appointed by the Online Safety Group. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person will be decided by the Online Safety Group
- be reported to the Online Safety Group every half term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the person appointed by the Online Safety Group any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

- *The school / academy maintains and supports the managed filtering service provided by the Internet Service Provider*
  In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / Principal (or other nominated senior leader).
- *Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school business manager will decide whether to make school level changes.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person appointed by the Online Safety Group
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

School Personal Data Advice and Guidance

Suggestions for use

This document is for advice and guidance purposes only.

School Personal Data Handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- No school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any-personal data breach.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.
- It is a legal requirement for all schools to have a Data Protection Policy.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in the school but also from remote locations. It is important to stress that the data protection laws applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority / Parent Organisation regulations and guidance and changes in legislation.

Introduction

Schools and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority / Parent Organisation).

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. This represents a significant shift in legislation and replaces the Data Protection Act 1998. The UK legislation was announced on the 14th September 2017. The Data Protection Bill's (DP Bill) journey through parliament and the associated text has been published online. The EU GDPR gives members states, like the UK, limited opportunities to make unique provision for how the regulation applies. However, the GDPR and the DP Bill should not be considered separately from each other.

Are schools in England and Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools and the personal data required in a variety of forms to operate a School this means that an educational college in the UK is required to comply.

Guidance for schools is available on the Information Commissioner's Office website including information about the new regulations.

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. Good advice would encourage the School to:

- Delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- Consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually

- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's publication scheme should be reviewed annually. The ICO produce guidance on the model publication scheme for schools. This is designed to support schools complete the Guide to Information for Schools.

Personal Data

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Fee

The School should pay the relevant fee to the ICO.

Responsibilities

Every maintained school in the UK is required to appoint a Data Protection Officer as a core function of 'the business' includes:

- regular and systematic monitoring of individuals on a large scale;
- [the processing of] special categories[2] of data on a large scale and data relating to criminal convictions and offences

The Data Protection Officer (DPO) can be internally or externally appointed.

[2] • 'Special categories of data' is the type of data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; genetic data, biometric data or data concerning health or sex life and sexual orientation

They must have:

- Expert knowledge
- Timely and proper involvement in all issues relating to data protection
- The necessary resources to fulfil the role
- Access to the necessary personal data processing operations
- A direct reporting route to the highest management level

The data controller must:

- Not give the DPO instructions regarding the performance of tasks
- Ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- Not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- Inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- Provide advice on a data protection impact assessment
- Co-operate with the Information Commissioner
- Act as the contact point for the Information Commissioner
- Monitor compliance with policies of the controller in relation to the protection of personal data
- Monitor compliance by the controller with data protection laws

The school may also wish to appoint a Data Manager. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Information to Parents / Carers – the Privacy Notice and Consent

In order to comply with the fair processing requirements in data protection law, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers for example in the prospectus, newsletters, reports or a specific letter / communication. Parents / carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

More information about the suggested wording of privacy notices can be found on the DfE website.

The DFE only publishes documents for England. But these template privacy notices may be suitable for amendment by schools in other UK nations.

Consent under the regulation has changed. Consent is defined as:

"in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. Pupils / students aged 13 or over (the age proposed in the Data Protection Bill, subject to Parliamentary approval) may be able to consent to their data being processed for the purposes of information society services. The GDPR does not specify an age of consent for general processing bur schools should consider the capacity of pupils to freely give their informed consent.

Schools should satisfy themselves that their consent forms are clear and written in plain language. Consent should also detail in a very clear and specific way why this is necessary, what will happen to the data, and, how and when it will be disposed of.

Consent is just one of the six lawful bases for processing data:

1. Consent:
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the

data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Previously maintained schools / academies were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools as defined in Schedule 1 of the Freedom of Information Act 2000 and referenced in the UK Data Protection Bill 2017). This now means that should you wish to process the personal data of a child a risk assessment must be completed and justification documented.

Data Protection Impact Assessments (DPIA)

According to the ICO, Data Protection Impact Assessments (DPIA): "help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy."

These will be carried out by Data Managers under the support and guidance of the DPO. These are intended to be carried out before processing activity starts, although some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks.

According to the ICO a DPIA should contain:

- A description of the processing operations and the purpose.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- Who did you talk to about this?
- What is going to happen with the data and how – collection, storage, usage, disposal
- How much personal data will be handled (number of subjects)
- Why you need use personal data in this way
- What personal data (including if it's in a 'special category') are you using
- At what points could the data become vulnerable to a breach (loss, stolen, malicious)
- What are the risks to the rights of the individuals if the data was breached
- What are you going to do in order to reduce the risks of data loss and prove you are compliant with the law

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Special categories of personal data

The following list is a list of personal data listed in the GDPR as a 'special category'.
"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities, through opportunities such as:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Secure storage of and access to data

The school / academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school / academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school / academy personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school / academy policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school / academy should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school / academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. The ICO produced guidance about cloud storage for organisations in 2012.

As a Data Controller, the school / academy is responsible for the security of any data passed to a "third party". Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Subject Access Requests

Data subjects have a number of rights in connection with their personal data:

- Right to be informed – Privacy notices
- Right of access – Subject Access Request
- Right to rectification – correcting errors
- Right to erasure – deletion of data when there is no compelling reason to keep it
- Right to restrict processing – blocking or suppression of processing
- Right to portability – Unlikely to be used in a School / Academy context
- Right to object – objection based on grounds pertaining to their situation
- Rights related to automated decision making, including profiling

Clearly several of these have the opportunity to impact on schools / academies, one being the right of access. Procedures must be in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. The school must provide the information free of charge, however a 'reasonable fee' may be charged where the request is manifestly unfounded or excessive, especially if this is a repetitive request. See later information on Records of Processing Activity.

Secure transfer of data and access out of school

The school / academy recognises that personal data may be accessed by users out of school / academy, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school / academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school / academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school / academy should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provide support for this process. The school / academy must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. This must include:

- The name and contact details of the data controller
- Where applicable, the name and contact details of the joint controller and data protection officer
- The purpose of the processing
- To whom the data has been/will be disclosed
- Description of data subject and personal data

- Where relevant the countries it has been transferred to
- Under which condition for processing the data has been collected
- Under what lawful basis processing is being carried out
- Where necessary, how it is retained and destroyed
- A general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the School / Academy to target training at the most at-risk data
- record any breaches that impact on the data

It then follows that in the event of a data breach, the school/ college should have a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedure
- and results in a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

Data Mapping

The process of data mapping is designed to help schools / academies identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your students then this processor has obligations on behalf of the school / academy to ensure that processing takes place in compliance with data protection laws.

Privacy and Electronic Communications

Schools / academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by:

Kerry Taylor - School Business Manager

Paul Knight –Assistant Headteacher

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

Jordan Griffin – IT co-ordination

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices

Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school. If brought in they are to be handed in at the beginning of each day to be collected at the end of the school day..

If pupils breach these roles:

The sanctions for breaking these rules can be found in the Behaviour Policy, ICT Policy & Anti Bullying policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the s pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm

will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do .

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

Audit / Monitoring / Reporting / Review

The school business manager will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by Online Safety Committee at regular intervals every meeting.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

https://www.gov.uk/government/publications/searching-screening-and-confiscation

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices will be school owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils, staff and wider school community understand that the primary purpose of having use of mobile devices and desktop computers at school is educational. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/advice/bring-your-own-device-byod

Considerations

Our current policy prohibits use of personal devices , should these be considered in the future ,the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[3]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No*	No**	No
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access				Yes	Yes	Yes

***if brought in they are to be handed in at the beginning of the day and collected at the end.**
**** to be stored in staffroom or other secure place and not to be used whilst working.**

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete / amend as appropriate):

[3] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

- All school devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.

- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school
  - Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
  - Devices must be in silent mode on the school site and on school buses
  - School devices are provided to support learning. It is expected that pupils/students will bring devices to school as required.
  - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
  - The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
  - The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
  - Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.

- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The Compass Learning Centre recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Organisational control

Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- Administrator / Moderator
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online

Personal use

- Staff.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - The school permits reasonable and appropriate access to private social media sites outside of working hours.
- Pupil/Students
    - Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- Parents/Carers
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

School Policy – Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the Compass Learning Centre community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- *Student / pupil representation* will be obtained from pupil voice meetings
- Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.2. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.3. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.4. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;

- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held every half term for a period of 1 hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:
- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for the Compass Learning Centre have been agreed

Signed by (SLT): .....

Date: .....

Date for review: .....

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to

imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data- http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guide for Organisations (general information about Data Protection)
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Computing
ICO - Guidance we gave to schools - September 2012
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Ofcom –Media Literacy Research

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Appendices

A. Online Contact with Students Regarding Academic Progress
B. Office 365 get started guide (students)
C. Office 365 get started guide (staff)
D. Esports Computer Protocols

A. Online Contact with Students Regarding Academic Progress

Pre meeting

1. Parents of students will be contacted prior to any contact to obtain permission for any meeting to take place. A record of the contact will be on SIMs and the response recorded on the Student Record of Online Contact (Academic)
2. Meetings will be scheduled in advance ideally at least 24 hours, a time will be set and if the student is not present at the meeting within 15 minutes of the start time the parent will be contacted by telephone to check all is well

Meeting structure

- Meetings can be up to but in most cases not more than 45 minutes
- There should be time set aside for catching up aside from academic work
- During the main body of the meeting it would be ideal if both the student and staff could have the work available to them
- Staff should also record an action plan for the student
- Set a time and date for a follow up meeting in a reasonable timeframe

Introduction – purpose of the meeting Quick catch up News	5 Mins
Main body – discuss work completed, look at work together and any new work set. Any questions about work set?	30 mins
Summary – Set targets before a follow up contact at a set date and time	10 mins
Remaining time can be used to share news	N/A

- If the student is not behaving appropriately during any meeting, then video should be turned off and the message "I am going to end this meeting now and arrange to meet another time"
- Staff should keep a log of the meeting to record in the Student Record of Online Contact (Academic)

Post meeting

1. Record details of the meeting on Student Record of Online Contact (Academic)
    a. If necessary highlight any issues from the meeting with the relevant staff member (subject teacher/safeguarding leads/Headteacher)
2. Share the action plan including targets based on the meeting content with the student by email and remind them of the plan to meet.
3. Share the scheduled meeting with parents and record on Student Record of Online Contact (Academic)

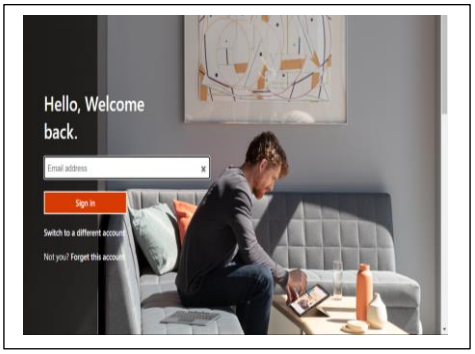
Live Learning: Code of Conduct

1. The purpose of any Compass led learning streams for lessons/tutorials/assemblies is to support students' learning, personal development or welfare
2. Although we are not in the same building, our normal rules apply: everyone must act with care, consideration, kindness and concern at all times
3. Live meetings will be recorded by the teacher for safeguarding and to simplify note taking
4. Students are not permitted to record live learning streams
5. Students should wear sensible clothing. Consideration should be given to appropriate clothing (e.g. shoulders covered)
6. Students should join the live stream in a shared space in the home and not in a bedroom if at all possible
7. Students should join the live learning stream 5 minutes before the published start time to check all of their settings are working correctly
8. Students must not join live stream lessons in public places outside of the family home
9. Teachers will admit students to the live learning stream one by one to check identification and welcome students
10. When joining the live learning stream, students' microphones and videos will be muted. Students should unmute their video feed briefly for identification purposes
11. If students wish to, they can join the stream by video fully by "enabling" their own video using the settings in MS Teams
12. If students do use a video stream, the following must apply about the video stream:

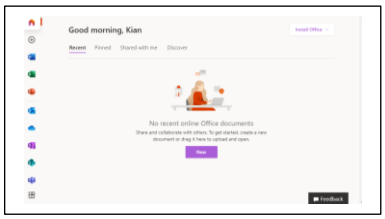
- The full face must be visible
- Head coverings (e.g. caps / hats) must not be worn (unless for religious purposes)
- Students must clearly focus on the lesson and not on distractions
- Preferably, a neutral background should be used
- Inappropriate images must not be visible in the background

13. Students may wish to join live learning streams by audio only and leave their video feed muted once identified by staff
14. The teacher delivering the lesson may be supported by at least one other member of staff
15. The supporting member of staff will act as a co-host to monitor online behaviour
16. There must be no inappropriate language used in the chat function
17. There must be no inappropriate gestures or images used or posted on the screen
18. Students should complete the tasks required following direction from the teacher
19. If students online behaviour is not appropriate, they will be removed from the meeting/the meeting will cease and we will contact parents to discuss a possible sanction in response to the behaviour

B. Office 365 get started guide (students)



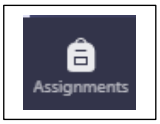
1. Login to https://www.office.com using your school email login details which will be provided
    a. Change your password, make sure you make a note of this somewhere, the password setup can be frustrating.....

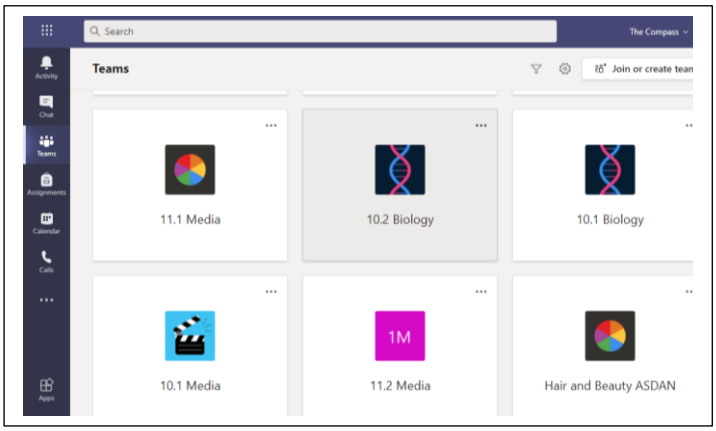


2. The site will offer to show you what it can do with some of the apps – it is up to you whether you go through these

3. From the screen above you have access to all of the Microsoft apps you will need on the left hand side of the screen
    a. Locate 'Teams' the one which looks like this

4. Here you will find the classrooms teachers have setup for you. You should have one for each subject you study
    a. You can explore a specific subject using its icon
    b. If you select the 'assignments' icon you can select the subject assignment



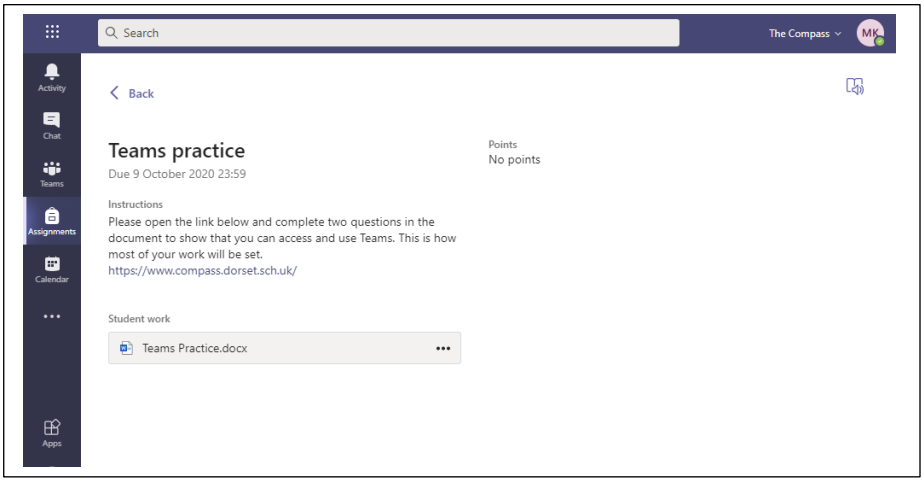


5. To practice find the team called 'Teams Practice'

    a. This icon from the 'Teams' screen and then select assignments

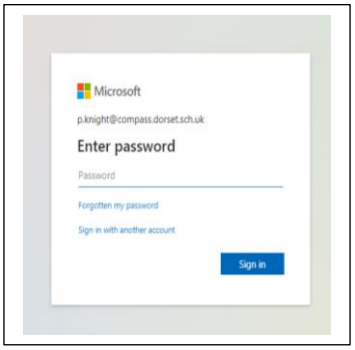
    b. This one from the 'Assignments' screen

6. Follow the instructions on this screen.



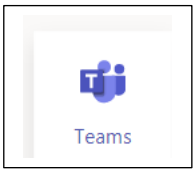
You are part of the online team!

c. Office 365 get started guide (staff)

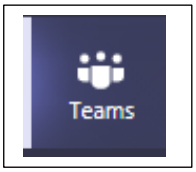


7. Login to https://www.office.com (your work email) using your school email login details

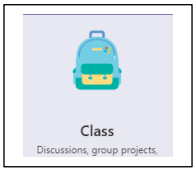
8. Click the Microsoft Teams app
- We will now set up a class team

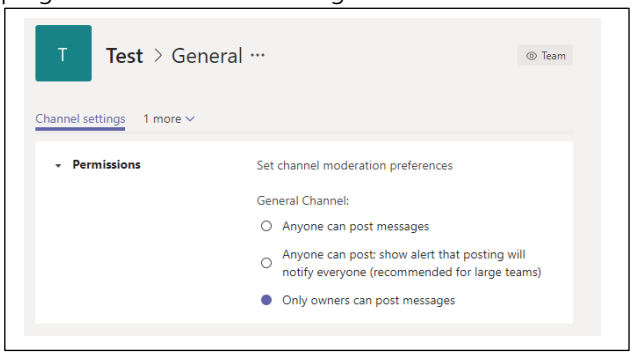


9. Click the Teams Tab



10. In the top right corner, click Join or Create Team
    a. On the next screen create a team
    b. Click the class option
    c. Choose one of your classes and type in the name (a description can be added later
    d. Add the students to the team, type their name and their school email address will appear
    e. Add staff who will need to be part of the teaching team. (All staff who teach this group this subject, subject leader, Emma, Paul, Mark, Alison & Becky)
    f. Before I congratulate you for creating a Team I think it best to point out you have control over who can post here
        i. Click the three dots in the top right corner and find manage channel
        ii. On this page select the option "Only owners can post messages"





You have created a team!

Setting Assignments for Students

1. Find your lesson on Oak Academy or however you are choosing to deliver input
    a. At this point you may wish to create your resource to work alongside this using word, excel or whatever format you choose. If doing this make sure it is available online.
2. Click on "3more", select assignments & then "create"
3. Click "assignment" and enter the title of your assignment
4. Enter the instructions for your assignment, this is probably the best place to add links to videos and other resources you would like students to view
5. Use the paperclip icon below to add the work you created earlier or create the work for the lesson at this point by selecting this option
    a. Click the 3 dots next to your uploaded document and select the option "students edit their own copy"
6. Enter your hand in date and time
7. Select "Assign"

You have created an assignment!

D. Esports Computer Protocols

1. Social Media. Avoid using any forms of social media apart from when using them for research purposes.
2. Inappropriate Websites. Avoid accessing any websites that would be seen to be inappropriate.
3. Web Browser. Avoid using the web browser for anything other than research purposes.
4. Offensive expression. Avoid expressing ourselves in an offensive manner toward other players or their actions in the game, regardless of whether they are opponents or teammates.
5. Offensive language. Avoid using language, nicknames or other expressions that insult another player's gender, gender identity, origin, physical ability, sexual orientation, religion or age.
6. Team dynamic. Always support your team, communicating positively and with respect.
7. Violent language. Avoid using language or actions that refer to sexual violence or other violence.
8. Violent actions. Avoid acting in a threatening or violent manner.
9. Cheating. Avoid cheating or hacking.
10. Private information. Avoid sharing our account information or any other private information that could put our peers or ourselves at risk.
11. Harassment. You may not harass other players, team members, or other associated parties.
12. Sexual Harassment. You may not sexually harass other players, team members or other associated parties. There is zero tolerance for any sexual threats or coercion or the promise of advantages in exchange for sexual favours.
13. Discrimination and Denigration. You may not offend the dignity or integrity of a country, private person, or group of people through contemptuous, discriminatory, or derogatory words in regards to race, ethnicity, socioeconomic status, ability status, gender identity, language, religion, political opinion or any other opinion, sexual orientation, or any other reason.

Dorset Council **Risk Assessment** **FORM 6**

Esports Computer Usage	Date of Assessment 14/06/21
Assessment completed by (Name) Jordan Griffin	Due for review 14/06/21
(Designation) Teaching Assistant	

Hazard / Risk Things at the venue, parts of the activity etc that could cause harm	**Who is at risk?**	**Current Controls in Place** Are they adequate? Is the risk acceptable? Refer to generic RAs or Form 2 if applicable	**Level of Residual Risk** Low, medium, high
Fluids and food in computer room	Students, staff	No drink or food will be allowed In the room. Drinks will be offered at break times and outside of the computer room. All students will be informed before entering the room.	Low
Equipment and furniture safety	Students, staff	Equipment being broken, damaged or not used for its purpose. Students will be reminded of consequences and sanctions regarding these actions.	Low
Electrocution	Students, staff	All equipment will be safety tested and staff will be vigilant of any damage.	Low
Fire	Students, Staff	See above. No plug sockets will be overloaded.	Low
Esafety	Students, public, staff	Students will be monitored at all times while using the esports computers. They will be reminded of consequences and sanctions. We will have a strict set of rules and protocols for esports computer usage.	Low