Chosen Hill School
E-Safety Protocol

Introduction

This Protocol applies to all members of Chosen Hill School's community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of School ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the School site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this Protocol, which may take place outside of the School, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Management Policy and Searching Screening and Confiscation Protocol

The School will deal with such incidents within this Protocol and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of School.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the School.

Governors:

Governors are responsible for reviewing the effectiveness of the Protocol. This will be carried out by the Community & People Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body in the Community & People Committee has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator (DSL)
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Community & People Committee

Headteacher and Senior Leadership Team:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the School community, the day to day responsibility for e-safety is shared between the Headteacher, the Designated Safeguarding Lead (Deputy Headteacher) and the Assistant Headteacher - Progress & Assessment.
- The Headteacher and the Designated Safeguarding Lead are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that she, the Designated Safeguarding Lead (E-Safety Coordinator) receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher and Business Manager will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal e-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 will receive regular monitoring reports on E-Safety as part of its monitoring and self-evaluation cycle.

E-Safety Coordination:

The Designated Safeguarding Lead & Assistant Headteacher (Progress & Assessment) will lead e-safety reporting as part of the senior team strategy meeting agenda. The Designated Safeguarding Lead, AHT and Business Manager will

- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the School e-safety documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the relevant body
- liaise with IT Services staff
- receives reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend Community & People meetings
- report regularly to Senior Leadership Team on e-safety issues through the senior team meeting structures
- E-Safety incidents will be reported to the Headteacher and dealt with in line with the School Behaviour Management policy including investigation, action and sanctions

IT Services Staff:

The Network Manager and Assistant Network Manager are 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 e-safety technical requirements and the E-Safety Protocol / Guidance.
- that users may only access the networks and devices through a properly enforced password protection Protocol, in which passwords are regularly changed
- the filtering Protocol, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Protocol Template" for good practice)
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or Designated Safeguarding Lead or Assistant Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in School documents

All Staff

All staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current E-safety Protocol and practices
- they have read, understood and signed the Staff Acceptable Use / Agreement
- they report any suspected misuse or problem to the Designated Safeguarding Lead / Assistant Headteacher for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official School systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use procedures
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. 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 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

The designated safeguarding lead, and any nominated deputy, will be trained in e-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
- cyber-bullying

Senior ICT Strategy Group

The work of the ICT Strategy Group will be part of the Senior Leadership Team planned programme. The ICT Strategy Group will consult with group appropriate staff and community representative from the School as part of carrying out its responsibility for issues regarding e-safety and the monitoring the E-safety Protocol including the impact of initiatives.

Members of the ICT Strategy Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the School e-safety Protocol.
- the production / review / monitoring of the School Filtering Protocol and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the e-safety provision

An ICT Strategy Group Terms of Reference Template can be found in the appendices (A)

Students:

Students are responsible for using the digital technology systems in accordance with the Student Acceptable Use Agreement and:

- 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of School and realise that the E-Safety Protocol 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 internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at School events
- access to parents' sections of the website and on-line student / student records (INSIGHT)
- their children's personal devices in the academy

Community Users

Community Users who access School's website as part of the wider provision will be expected to sign a Community Acceptable User Agreement (see page 22) before being provided with access to School systems.

Education and Training

Students

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

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

- A planned e-safety curriculum is provided as part of the ICT and CPHSE lessons and is regularly revisited in other lessons as appropriate to the teaching focus
- Key e-safety messages are reinforced as part of a planned programme of Learning Mentor/ pastoral activities
- Students are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside School
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned. It is recognised as best practice that students 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 students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Parents / carers

Many parents and carers have only a limited understanding of e-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 on-line 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 therefore seeks to provide information and awareness to parents and carers through:

- 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. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

The Wider Community

The School aims to provide opportunities for local community groups to gain from the School's e-safety knowledge and experience. This may be offered through the following:

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

Staff / Volunteers

All staff will receive e-safety training and understand their responsibilities, as outlined in this Protocol. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training will be carried out regularly
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the School e-safety Protocol and Acceptable Use Agreements**.**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety Protocol and its updates will be located on the L drive and available in hard copy to all new staff.
- The E-Safety Coordinator will provide guidance to individuals as required.

Training – Governors

Governors will take part in e-safety training and awareness sessions, for those involved in health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by a relevant group organisation.
- Participation in School training or information sessions for staff or parents.

Technical
Infrastructure / equipment, filtering and monitoring

The School will be responsible for ensuring that the School infrastructure and network is as safe and secure as is reasonably possible and that the procedures approved within this Protocol are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

A more detailed Technical Security Template Protocol can be found in the appendix.

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements**.**
- There will be regular reviews and audits of the safety and security of technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.
- The Domain Administrator password for the ICT system, will not be used on a day-to-day basis, but is available to the Headteacher / Designated Safeguarding Lead and kept in the School safe for emergency use
- The 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Academy 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 or potential technical security breach to the relevant person.
- 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 Protocol is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the School systems.
- An agreed Protocol is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on School devices that may be used out of School.
- An agreed Protocol is in place that allows staff to / forbids staff from downloading executable files and installing programmes on School devices.
- An agreed Protocol is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on School devices. Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured. Please see the Data Protection Policy for further information.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by the School of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that needed to be reviewed prior to implementing such a Protocol. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive - see BYOD Protocol.

- The School has a set of clear expectations and responsibilities for all users
- The School adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the School's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD Protocol
- Any user leaving the School will follow the process outlined within the BYOD Protocol

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 students about the risks associated with the taking, using, 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.
- 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).
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Where practical School equipment should be used for photographs and videos. In the event that personal equipment is used (this includes SD cards, memory sticks, CDs etc...) they should only provide a temporary storage medium. Once the media are uploaded to the appropriate area of the School network, images should be erased from their initial storage location.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names may be used on a website, blog, or social media account with parental permission when associated with photographs.
- Permission from parents or carers will be obtained before photographs of students are published on the School website (covered as part of the AUA signed by parents or carers at the start of the year.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

The Schools Data Protection Policy is available to all staff on the VLE.

Communications

This is an area of rapidly developing technologies and uses. The School continues to discuss and agree how it intends to implement and use these technologies. 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			Students				
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 to School	x				x			
Use of mobile phones in lessons		x					x	
Use of mobile phones in social time	x				x			
Taking photos on mobile phones / cameras		x				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				
Use of messaging apps		x				x		
Use of social media		x				x		
Use of blogs		x					x	

When using communication technologies, the School considers the following as good practice:

- The official academy email service may be regarded as safe and secure and all users should be aware it is monitored. All email communication between staff and students should only be via the Academy's email system.
- Users must immediately report, to the nominated person – in accordance with the academy Protocol, 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.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- No personal information of staff other than name and official email address should be posted on the School website.

Social Media

The School's Social Media Protocol is available on the VLE.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy 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 the 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 School or outside School when using School equipment or systems. The School Protocol 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,	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

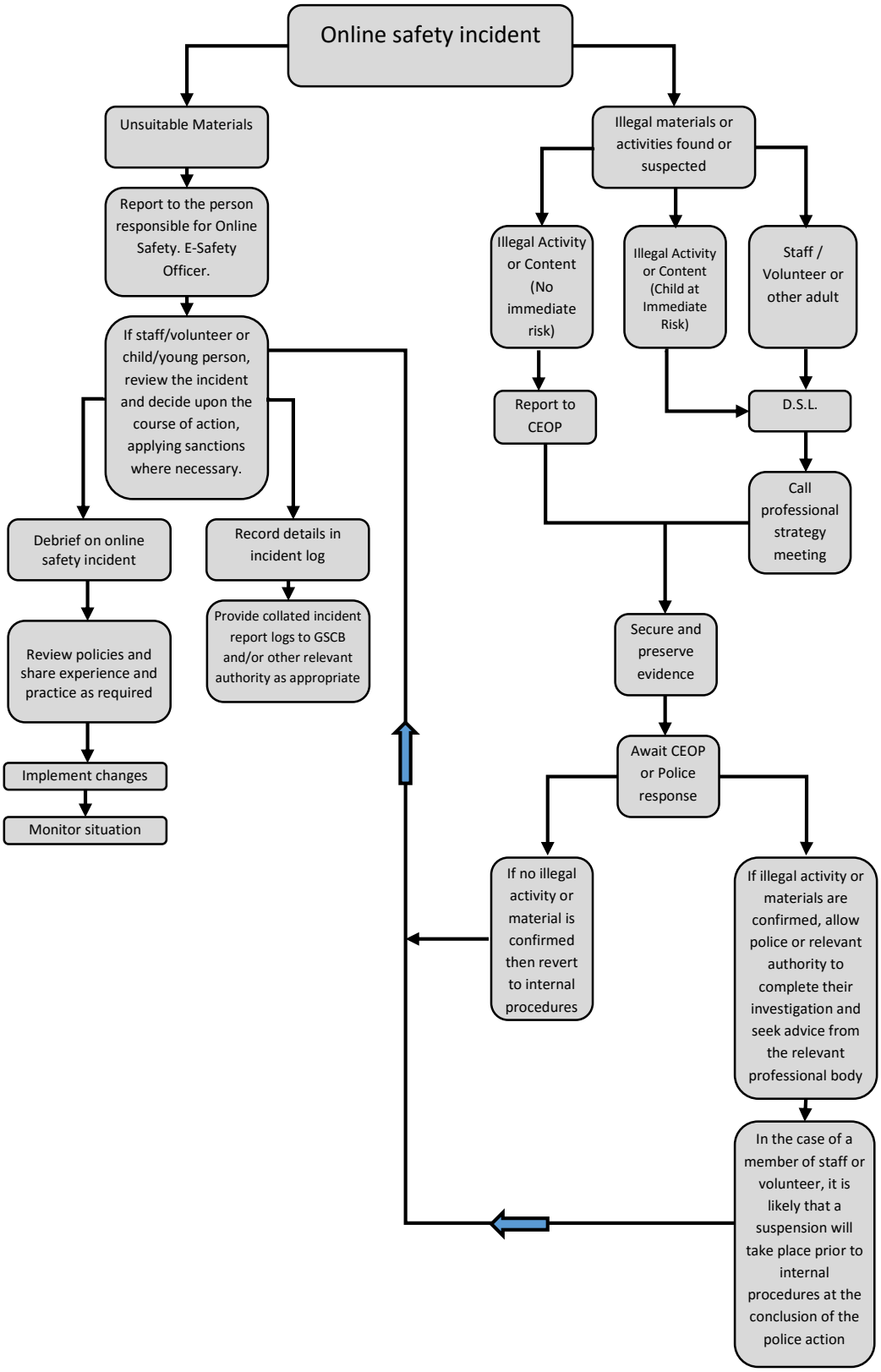
proposals or comments that contain or relate to:	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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 academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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			

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).

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 immediately to the Safeguarding flow chart for responding to online safety incidents and report immediately to the School's Designated Safeguarding Lead and the police.


Online safety incident
Unsuitable Materials
Report to the person responsible for Online Safety. E-Safety Officer.
If staff/volunteer or child/young person, review the incident and decide upon the course of action, applying sanctions where necessary.
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to GSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff / Volunteer or other adult
Report to CEOP
D.S.L.
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the School community will be responsible users of digital technologies, who understand and follow this Protocol. However, there may be times when infringements of the Protocol 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 member of the senior leadership team (Headteacher or DSL or AHT) staff / volunteer 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 investigating officer 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
- Police involvement and/or action

If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Designated Safeguarding Lead immediately. Other instances to report 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
- other criminal conduct, activity or materials

Ensure you isolate the computer in question as best you can, as 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 academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Actions and 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:

Students Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / LL	Refer to Head Teacher	Refer to Police	Refer to I.T. technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. 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					
Unauthorised use of non-educational sites during lessons	X	X				X	X	X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X			
Unauthorised use of social media / messaging apps / personal email	X	X			X	X	X	X	X
Unauthorised downloading or uploading of files	X	X				X	X	X	X
Allowing others to access the network by sharing username and passwords	X	X	X		X	X	X	X	X
Attempting to access or accessing the network, using another student's account	X	X			X	X	X	X	X
Attempting to access or accessing the network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions	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	X	X
Using proxy sites or other means to subvert the School's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		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	

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Business Manager	Refer to Local Authority / HR	Refer to Police	Refer to I.T. 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				
Inappropriate personal use of the internet / social media / personal email	X	X	X		X	X		
Unauthorised downloading or uploading of files	X	X	X		X	X		
Allowing others to access the network by sharing username and passwords or attempting to access or accessing the network, using another person's account	X	X	X			X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X
Using personal email / personal social networking / personal instant messaging / personal text messaging to carrying out digital communications with students	X	X	X					X
Actions which could compromise the staff member's professional standing	X	X	X			X		X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	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
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X				X	X
Breaching copyright or licensing regulations	X	X	X			X		X
Continued infringements of the above, following previous warnings or sanctions		X	X		X			X

Student Acceptable Use Protocol Agreement

Introduction

Digital technologies have become integral to the 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.

The Student Acceptable Use Protocol is intended 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 users at risk.

The School will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that Chosen Hill 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.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- 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 Chosen Hill 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 academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards 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 integrity of the technology it offers me and to ensure the smooth running of the School:

- I will only use my own personal devices (mobile phones / USB devices etc.) in School if I have permission. I understand that, if I do use my own devices Chosen Hill School, I will follow the rules set out in this agreement, in the same way as if I was using School equipment.
- 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 will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 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 social media sites with permission and at the times that are allowed .

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 Chosen Hill 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 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.

This form relates to the student 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 ICT systems.

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

- I use Chosen Hill School systems and devices (both in and out of School)
- I use my own devices in Chosen Hill School (when allowed) e.g. mobile phones, USB devices, cameras etc.
- I use my own equipment out of the School in a way that is related to me being a member of this School e.g. communicating with other members of the School, accessing School email, VLE, website etc.

Name of Student	
Learning Mentor Group	
Signed	
Date	

Parent / Carer Countersignature

Name of Parent / Carer	
Signed	
Date	

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students 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 in the public media.

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 students in the digital / video images.

The School's Admission form contains a section regarding this matter and requests permission to allow the School to take and use images.

Staff (and Volunteer) Acceptable Use Protocol

Staff Acceptable Use Agreement

I understand that I must use School ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of School ICT systems (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 ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within E1 and C Protocol and rules set down by the School.
- I will not disclose my username or password to anyone else (except in rare circumstance and only to Senior IT staff), 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 Protocol on the use of digital / video images.
- I will not use chat and social networking sites in School in accordance with the School's policies.
- I will only communicate with students and parents / carers using official School systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the School:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in School, I will follow the rules set out in this agreement, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- 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 on portable media 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 Personal Data Protocol (or other relevant Protocol). 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.
- School laptops will be provided with an encrypted partition which must be used for all personal data.
- I understand that data protection Protocol requires that any staff or student 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 Protocol 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.

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 Protocol applies not only to my work and use of academy ICT equipment in School, but also applies to my use of School ICT 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 Protocol Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 ICT 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	

Community Users Acceptable Use Protocol

This Acceptable Use Protocol 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 Chosen Hill School's 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 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

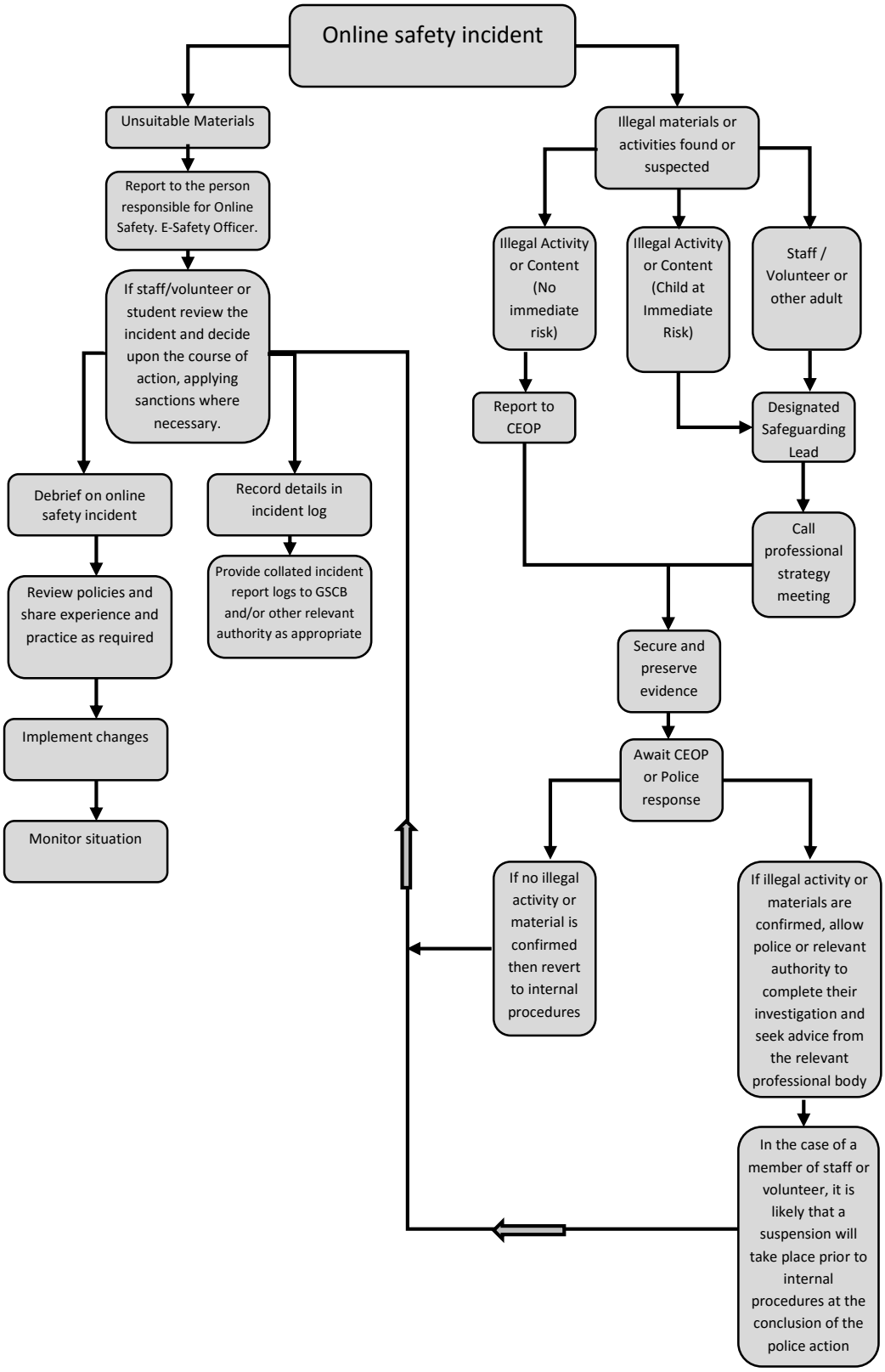
I have read and understand the above and agree to use the School ICT systems (both in and out of School) and my own devices (in School and when carrying out communications related to the School) within these guidelines.

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

Template Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Training Needs Audit

Training Needs Audit Log

Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

School Technical Security Protocol (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 procedure
- 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 Protocol and practice.

Responsibilities

The management of technical security will be the joint responsibility of the Senior IT Technicians.

Technical Security

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 Protocol are implemented. It will also need to ensure that the relevant people will 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. Details of the access rights available to groups of users will be recorded by the Senior IT Technician and will be reviewed, at least annually, by the E-Safety Officers.
- 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.
- The Senior IT Technician 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 installation
- 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 Agreements.
- Remote management tools are used by staff to control workstations and view users' activity
- An agreed procedure is in place for the provision of temporary access of "guests" onto the School system

- An agreed procedure is in place for the provision of trainee teachers and supply teachers onto the school system.
- An agreed protocol is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on School devices that may be used out of School.
- An agreed protocol is in place within the Data Protection Protocol regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on School devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data should not be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is in place and for all School technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Protocol Statements

- All users have clearly defined access rights to School technical systems and devices. Details of the access rights available to groups of users are recorded by the E-Safety Coordinator with the senior IT Technician and will be reviewed, at least annually, by the E-Safety Coordinator.
- All academy networks and systems will be protected by secure passwords that are regularly changed**.**
- The "master / administrator" passwords for the academy systems, used by the technical staff are also be available to the Headteacher / Designated Safeguarding Lead/Business Manager and kept in a secure place e.g. School safe. Two factor authentication is under development for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by the I.T. Technical staff.
- 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.
- Users will change their passwords at regular intervals – as prompted by the system.
- The level of security required may vary for staff and student accounts and the sensitive nature of any data accessed through that account.
- requests for password changes will be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following three successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of School
- should be changed at least every 6 months. The frequency may increase dependent on the nature of the account and how sensitive / damaging loss of data would be.
- the last ten passwords cannot be re-used passwords created by the same user.
- should be different for systems used inside and outside of School

Student passwords

- All users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames.
- Users will be required to change their password every 6 months.
- Students will be taught the importance of password security

Training / Awareness

Users will be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Members of staff will be made aware of the School's password procedure:

- at induction
- through the School's e-safety Protocol
- through the Acceptable Use Agreement

Students will be made aware of the School's password procedure:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The senior IT Technician will ensure that full records are kept of:

- User IDs and latest request for password changes
- User log-ons
- Security incidents related to this Protocol

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 e-safety and acceptable use.

Staff are made aware of the flexibility provided by the filtering services at the School. The School uses this flexibility to meet student and staff learning needs and reduces some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.
The School will:

- Use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for the School.
- Introduce differentiated filtering for different groups / ages of users
- Remove filtering controls for some internet use at certain times of the day or for certain users.

Responsibilities

The responsibility for the management of the School's filtering Protocol will be held by the Senior IT Technician. They will manage the School filtering, in line with this Protocol 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 are:

- logged in change control logs

- are reported to a second responsible person who is nominated as an E-Safety Officer
- is reported to the senior ICT strategy review group annually
- All users have a responsibility to report immediately to the Senior IT Technician any infringements of the School's filtering Protocol 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.

Protocol 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 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. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the School network, filtering will be applied that is consistent with School practice.

- In the event of the technical staff needing to switch off all filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / Business Manager.
- Mobile devices that access the academy internet connection (whether 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 senior ICT strategy committee.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme within their ICT and CPSHE lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

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

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

Parents will be informed of the School's filtering Protocol through the Acceptable Use Agreement and through e-safety briefing information.

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 E-Safety Protocol and the Acceptable Use Agreement. Monitoring will take place as follows:

Audit / Reporting

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

- ICT Strategy Group

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

Personal Data Handling Protocol

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. 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, and/or
- 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 Commissioners Office for the School and the individuals involved. 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 this Protocol, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines “Sensitive Personal Data” as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Protocol Statements

The School 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.
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see Privacy Notice)

Personal Data

The School and individuals 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 students, 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 / student 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.

Responsibilities

The School's Senior Information Risk Officer (SIRO) is the Assistant Headteacher (Data). This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the School's information risk Protocol and risk assessment
- appoint the Information Asset Owners (IAOs)

The School will identify Information Asset Owners (IAOs) who will be members of SLT with responsibility for key areas for the various types of data being held (e.g. student information / staff information / assessment data etc.). The IAOs 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 protected 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 Protocol in the event that they have access to personal data, when engaged in their role as a Governor.

Training & awareness

All staff will receive data handling awareness and data protection training and will be made aware of their responsibilities, as described in this Protocol during the induction programme:
In addition, training and awareness raising will be delivered through:

- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions:

- The Hazard

- The control measure in place
- Any additional control measures that can be implemented

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to Schools?
NOT PROTECTIVELY MARKED	0	Will apply in Schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in Schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most student or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICTED.

The School will ensure that all School staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. “Securely delete or shred this information when you have finished using it”.

Schools will need to review the above section with regard to DfE and legal policies, which may be more specific, particularly in the case of employment records.

Secure Storage of and access to data

The School will ensure that ICT 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.

All users will use strong passwords which must be changed regularly in line with the School timelines.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access 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 can only be stored on School equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of 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 School has a data storage protocol.

The academy has clear Protocols and procedures for the automatic backing up, accessing and restoring all data held on School systems, including off-site backups.

The academy has clear an agreed Protocol for the use of “Cloud Based Storage Systems” (for example dropbox, google apps and google docs) 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 will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see appendix for further information and the ICO Guidance:
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

As a Data Controller, the academy is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The academy recognises that under Section 7 of the DPA,
http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are 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. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of School

The School recognises that personal data may be accessed by users out of School, 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 or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA / School policies may forbid such transfer);
- 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
- 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; and
- 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. (nb to carry encrypted material is illegal in some countries)

Disposal of data

The School will comply with the requirements for 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 overwritten, in accordance with government guidance (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

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

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals – Business Manager or AHT Data.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use Protocol, for example.
The School has an agreed Protocol for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and

- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling Protocol and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as School websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically Schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the School may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, School closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by Schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, Schools should not send detailed personally identifiable information. General, anonymous alerts about Schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues / documents related to Personal Data Handling in Schools:

Use of Cloud Services

Many Schools now use cloud hosted services. This section is designed to help you to understand your obligations and help you establish the appropriate policies and procedures when considering switching from locally-hosted services to cloud-hosted services.

What policies and procedures should be put in place for individual users of cloud-based services?

The School is ultimately responsible for the contract with the provider of the system, so check the terms and conditions carefully; below is a list of questions that you may want to consider when selecting a cloud services provider; indeed, you may want to contact any potential provider and ask them for responses to each of the following:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

SWGfL provides a useful summary of these issues in a document that has been written with the support of Google and Microsoft:

http://www.swgfl.org.uk/News/Content/News-Articles/Cloud-based-products-and-services

The document focusses on Google Apps for Education and Microsoft 365, but poses important considerations if a School is considering services from another provider.

Parental permission for use of cloud hosted services

Schools that use cloud hosting services (e.g. Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a School to obtain 'verifiable parental consent'. Normally, Schools will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template").

A template form has been added to the Parents & Carers Acceptable User Template elsewhere in these Template Policies.

Freedom of Information Act

For further information, please refer to the School's Freedom of Information Policy.

Model Publication Scheme

The Information Commissioners Office provides Schools with a model publication scheme which they should complete. This was revised in 2009, so any School with a scheme published prior to then should review this as a matter of urgency. The School's publication scheme should be reviewed annually.

Guidance on the model publication scheme can be found at:
http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx

Guidance and a Model Publication Scheme for Academies can be found at:
http://www.education.gov.uk/Schools/leadership/typesofSchools/academies/open/a00205178/freedom-of-information-guide-for-academies

Electronic Devices - Searching & Deletion

No existing law or Protocol can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others.

Background

The changing face of information technologies and ever increasing student 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 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 Protocol can on its own guarantee that the School will not face legal challenge, but having a robust Protocol 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 Protocol 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 School Behaviour Management policy which is available on the School's website.

Relevant legislation:

- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012

Responsibilities

The Headteacher is responsible for ensuring that the School policies reflect the requirements contained within the relevant legislation.

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: who should this be?

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

Training / Awareness

It is essential that all staff should be made aware of and should implement this procedure which is included within the E-Safety Protocol and is available in the Staff Handbook.

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 provided to those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Protocol Statements

Search:

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

The School's Policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions detailed in the Behaviour Management Policy and the Mobile Phone Use Protocol.

Authorised staff detailed 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 student's consent for any item.
- Searching without consent - Authorised staff may only search without the student'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 student is in possession of a prohibited item i.e. an item banned by the School rules and which can be searched for. Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training.

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 powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of students.

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 student being searched.

The authorised member of staff carrying out the search must be the same gender as the student 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 student being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student 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 student 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 student's possessions can only be searched in the presence of the student 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 so (i.e. the 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 break the School rules).

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

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The School should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff.

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. (i.e. the 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 break the School rules).

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. (It is recommended that members of staff should know who to contact, within School, for further guidance before taking action and that the person or persons is or are named within this Protocol).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the School can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the School to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

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 (particularly given the possible high value of some of these devices).

Audit / Monitoring / Reporting / Review

The responsible person 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 the ICT Strategy group three times a year.

School Bring Your Own Devices (BYOD) Template Protocol

To be added in line with Gloucestershire schools and GDPR compliancy

Appendix A

ICT Strategy Group Terms of Reference

1. PURPOSE

To provide a strategic group that has, as appropriate, representation from the academy community, with responsibility for issues regarding e-safety and the monitoring the e-safety Protocol including the impact of initiatives. The group is also responsible for regular reporting to the Full Governing Body.

2. MEMBERSHIP

2.1 The ICT Strategy Group will seek to include representation from all stakeholders as relevant to areas of focus and agenda items.
The composition of the group may include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinators
- ICT Technical Support staff

2.2 Other people may be invited to attend the meetings at the request of the Principal on behalf of the group to provide advice and assistance where necessary.
2.3 Group members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
2.4 Group members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
2.5 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. HEADTEACHER WILL LEAD THE MEETINGS INCLUDING:

- Scheduling meetings and notifying group members;
- Inviting other people to attend meetings when required by the group;
- 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 termly. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-ordinators with the following:

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review the e-safety Protocol in line with new technologies and incidents

- To monitor the delivery and impact of the e-safety Protocol
- To monitor the log of reported e-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 e-safety. This could be carried out through:
    - Staff meetings
    - Student forums (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for students, parents / carers and staff
    - Parents evenings
    - Website/VLE/Newsletters
    - E-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

Appendix B

Legislation

Schools should be aware of the legislative framework under which this E-Safety Protocol 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 Harassment 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 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

The new 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 Principals, to such extent as is reasonable, to regulate the behaviour of students 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 Principals (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template Protocol in these appendices and for DfE guidance - 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:
http://www.education.gov.uk/Schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoSchoolinformationregulations

Glossary of terms

AUP	Acceptable Use Protocol – 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.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	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 e-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

Development / Monitoring / Review of this Protocol

This e-safety Protocol has been developed by SLT and the IT Strategy Group made up of:

- Headteacher / Senior Leaders
- E-Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Community & People Committee
- Parents and Carers

Consultation with the whole School community has taken place through a range of formal and informal meetings.