EDEN PARK HIGH SCHOOL

DIGITAL CITIZENSHIP ONLINE SAFETY POLICY

Date of Last Review: January 2017

Date of Next Review: January 2019

Responsibility: Mrs E. Codling

Advisory Body Signature:

E21C
EDUCATION FOR THE 21ST CENTURY

Contents

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

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

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

This Policy has been reviewed in the light of the KCSIE Sept 2016 document.

Scope of the Policy

This policy applies to all members of Eden Park High School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital media (ICT) systems, both in and out of Eden Park High 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 disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Digital Citizenship Safety incidents covered by this policy, 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 for Learning Policy.

Eden Park High School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Digital Citizenship Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the digital citizenship safety roles and responsibilities of individuals and groups within the school.

Governors / Board of Directors:

Governors/Directors are responsible for the approval of the Digital Citizenship and Digital Citizenship Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/Directors receiving regular information about digital citizenship safety incidents and monitoring reports. A member of the Board has taken on the role of Safeguarding Director. The role of the Digital Citizenship Safety Governor/Director will include:

- regular meetings with the Digital Citizenship Co-ordinator
- attendance at Digital Citizenship Group meetings
- regular monitoring of digital citizenship safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Board meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including digital citizenship safety) of members of the school community, though the day to day responsibility for digital citizenship safety will be delegated to the Digital Citizenship Safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious digital citizenship safety allegation being made against a member of staff.
- The Headteacher is are responsible for ensuring that the Digital Citizenship Safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their digital citizenship safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal digital citizenship 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 from the Digital Citizenship Safety Co-ordinator.

Digital Citizenship Safety Coordinator/Officer:

- leads the Digital Citizenship Safety Group

- takes day to day responsibility for digital citizenship safety issues and has a leading role in establishing and reviewing the school's digital citizenship safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of a digital citizenship safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/relevant body
- liaises with school technical staff
- receives reports of digital citizenship safety incidents and creates a log of incidents to inform future digital citizenship safety developments
- meets regularly with Digital Citizenship Safety Director to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors/Directors
- reports regularly to Senior Leadership Team and DHT Safeguarding

Network Manager / Technical staff:

The Network Manager/Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required digital citizenship safety technical requirements of KCSIE 16, BSCB and LSCB.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with digital citizenship safety technical information in order to effectively carry out their digital citizenship safety role and to inform and update others as relevant
- that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader; Digital Citizenship Safety Coordinator for investigation.
- that monitoring systems are implemented currently the school I using Securus.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of digital citizenship safety matters and of the current school Digital Citizenship Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Digital Citizenship Safety Coordinator/appropriate pastoral leader for investigation
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- digital citizenship safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Digital Citizenship Safety Policy and acceptable use policies
- 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

Should be trained in Digital Citizenship 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

Digital Citizenship Safety Strategy Group

The Digital Citizenship Safety Strategy Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding

digital citizenship safety and the monitoring the Digital Citizenship Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Advisory Body.

Members of the Digital Citizenship Safety Group (or other relevant group) will assist the Digital Citizenship Safety Coordinator (or other relevant person, as above) with:

- the production/review/monitoring of the school Digital citizenship Safety Policy/documents.
- the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the digital citizenship safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the students about the digital citizenship safety provision

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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 digital citizenship safety practice when using digital technologies out of school and realise that the school's Digital Citizenship Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the 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/Learning Platform and information about national/local digital citizenship safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good digital citizenship safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' and students' sections of the website
- protocol where students hand in mobile phones at the beginning of each day

Policy Statements

Education – 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 digital citizenship safety is therefore an essential part of the school'sdigital citizenship safety provision. Children and young people need the help and support of the school to recognise and avoid digital citizenship safety risks and build their resilience.

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

- A planned digital citizenship safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key digital citizenship safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students should be 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 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 should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can

request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of digital citizenship 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 will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Web site
- Parents / Carers evenings / sessions – update 9, 10, 12 (training in Year 6)
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and digital citizenship safety
- Digital citizenship safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide digital citizenship safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Child-minders, youth/ sports/voluntary groups to enhance their Digital Citizenship Safety provision
- Primary schools, intend and extend to the E21C trust Digital Citizenship Ambassadors

Education & Training – Staff/Volunteers

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

- A planned programme of formal digital citizenship safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the digital citizenship safety training needs of all staff will be carried out regularly.
- All new staff should receive digital citizenship safety training as part of their induction programme, ensuring that they fully understand the school Digital Citizenship Safety Policy and Acceptable Use Agreements.
- The Digital Citizenship Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events.
- This Digital Citizenship Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days. Safeguarding including e-safety has a designated day every year, an update day and a whole-trust training day.
- The Digital Citizenship Safety Coordinator/Officer (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors/Directors

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

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation such as John Guest Safeguarding.
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school/technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT technician 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 6 months.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

- The 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 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. This is currently monitored by pastoral staff through Securus software.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (AUP) 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 policy is in place (AUP) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (AUP) regarding the use of removable media (eg 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.

Mobile Technologies (including BYOD/BYOT)

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

KS3 and KS4 hand in devices at the start of the working day.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour for Learning Policy, Bullying Policy, Acceptable Use Policy and all other relevant policies. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Digital Citizenship Safety education programme.

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, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press. This is included in the parts prior to Year 7 and Year 12 and for in-year admissions.
- 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.
- 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. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that 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 will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- 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".
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

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

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

Communications

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about digital citizenship safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority group liable to the injured party. Reasonable steps to prevent predictable harm must be in place. Staff are asked to consider if whether any material they publish on social media could compromise them in the future; if so, or if unsure, then they should not publish it.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in digital citizenship discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- An AUP for users of the accounts, including:
  - systems for reporting and dealing with abuse and misuse
  - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

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

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Digital Citizenship Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X

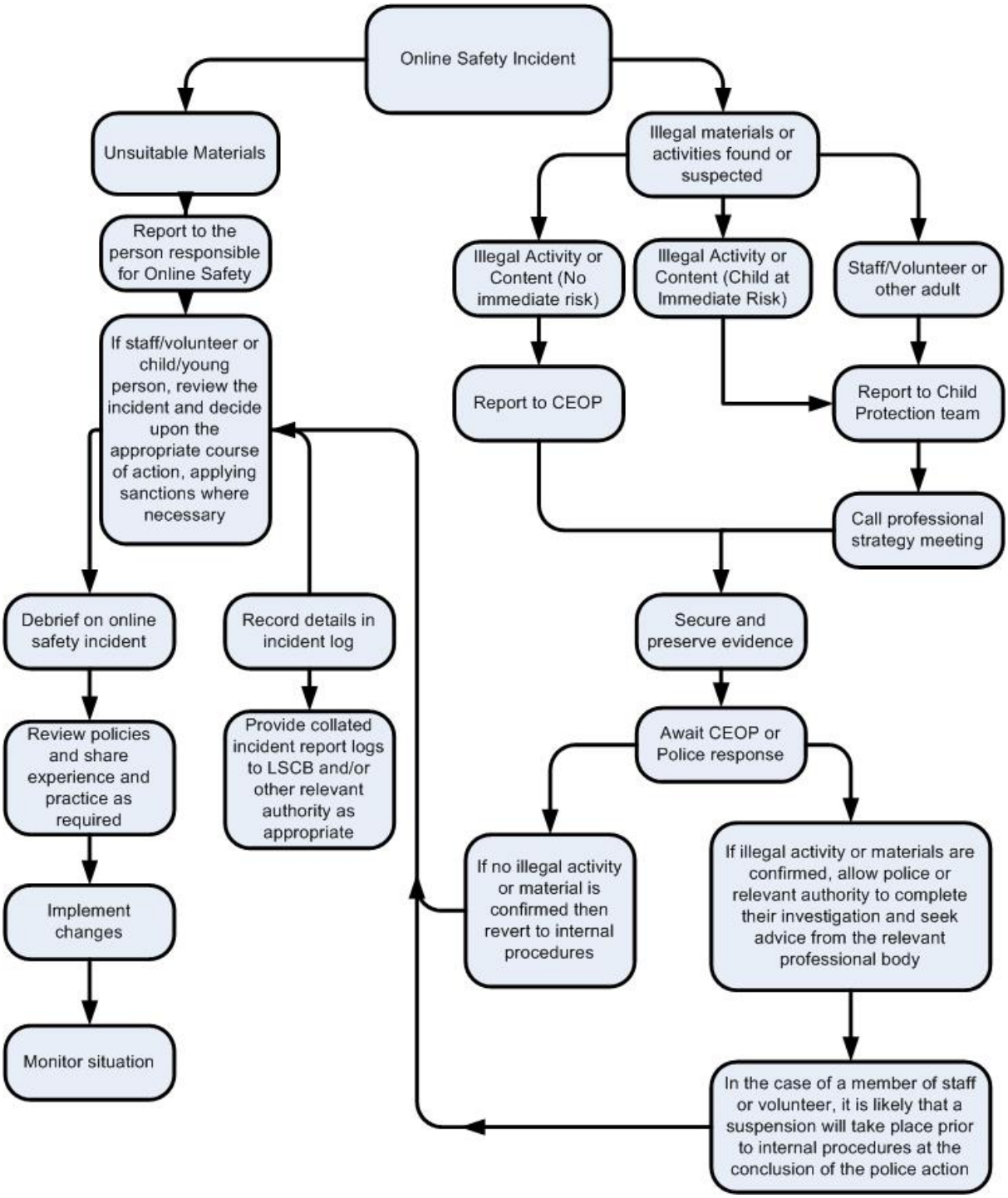
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)						
On-line gaming (non-educational)						
On-line gambling						
On-line shopping / commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting e.g. YouTube						

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of digital citizenship 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 to the right hand side of the Flowchart (below and appendix) for responding to digital citizenship safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. This part of the Policy should also consider the Complaints Procedure and Staff Code of Conduct.

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

- Have more than one senior member of 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 group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

Appendix

Acknowledgements

Appendices

Student Acceptable Use Agreement Template – The Acceptable Use Policy for Students

This policy covers use of digital technologies within Eden Park High School (EPHS) and when using EPHS Systems/Facilities: i.e. e-mail, Internet, Intranet and network resources, mobile phones, virtual learning environments, software applications, ICT equipment and ICT systems and smart devices i.e. smart watches.

- You must report to a teacher at school if, when using any form of digital technology, you:
  - have been threatened, intimidated, bullied, or upset, by anything received via, or created by, digital technology
  - have been contacted by another person asking you to give them personal or embarrassing information, including photographs
- You will only use the account and password given to you to access the schools network and facilities.
- Be aware that your activities whilst accessing and using the school network system is monitored and recorded.
- You will always log off or lock your computer (workstation) anytime you finish using a computer or leave your computer unattended.
- You are responsible for all activities that take place on your account if a computer (workstation) you are working on is not logged off or locked when left unattended.
- You will not share your network password with anybody.
- You will not write your password down.
- You will not use other persons username and/or password to access the school system.
- You will not use computers that have been left logged on by others.
- You will make sure that your password is at least 8 characters long and contains at least one capital letter and one number.
- You must only view and use websites and material that is needed for your school work.
- You are responsible for all e-mail messages sent from your account.
- You will never send anonymous messages or forward chain letters.
- You will always make sure that you communicate using professional, appropriate and respectful language.
- You must not attempt to gain access to any computer system, network, data, or resources you do not have permission to.
- You will not use the schools facilities for personal financial gain, gambling, political purposes or advertising.
- You will not try to bypass the internet filtering system to gain access to any website that would be normally blocked.
- You will not link your school email address to any social networking site.
- You will not download or install any software from the Internet.
- You understand that what you do on the Internet and on the school network is monitored, recorded and can be inspected if required.
- You will not access or attempt to access any type of on-line chat facility except those authorised by the school.
- You will not look through, download or send material that could be considered offensive/upsetting. (*The Headteacher holds the final decision on that which is considered offensive/upsetting).*
- You will not interfere with, or delete, the work of other students and teachers.
- You will not make or distribute any images, sounds, messages or other materials which are obscene, harassing, racist, inflammatory, malicious, fraudulent or libellous.
- You will not use any digital technologies in any way that would bring the name of school into disrepute.

- You will not interfere with the functioning of the school's network or any other network that can be accessed through the Internet.
- You understand that any activity that threatens, or is damaging to the school ICT systems, or that attacks or corrupts other systems, is forbidden.

We can only grant access to the school's ICT Systems/Facilities once a signed copy of the Acceptable Use Policy for Students has been received.

- I understand what digital technologies I am permitted to use at Eden Park High School.
- I agree to abide by this Acceptable Use Policy, and any reasonable revisions hereafter and which will be made public.
- I wish to have an email account, be connected to the Intranet and Internet and be able to use the school's ICT resources and systems.
- I understand the school reserves the right to examine or delete any files that may be held on, or run via its computer systems, or to monitor any Internet sites visited.

Full Name (Please print) ..... Year/Form .....

Student's Signature (dd/mm/yyyy) ..... Date .....

Parent/Guardian's Signature (dd/mm/yyyy) ..... Date .....

Office Use Only

Authorising Person (tick)

Digital Citizenship (e-Safety) coordinator ◯

Network Manager ◯

Form Tutor ◯

I approve this user access to EPHS Systems and Resources and for him/her to be set-up with a user account.

Signature ..... Date .....

Staff (and Volunteer) Acceptable Use Policy
Acceptable Use Policy for Staff 2017

NAME (PRINT/BLOCK CAPS)	

This policy covers use of digital technologies within Eden Park High School (EPHS) and when using EPHS Systems / Facilities: i.e. e-mail, Internet, Intranet and network resources, mobile phones, virtual learning environments, software, ICT equipment and ICT systems.

- I will only use the school's digital technology resources and systems for professional/work-related purposes, or for uses deemed to be 'reasonable' by the Headteacher.
- I will only use the approved, secure email system for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues or students *(The Headteacher holds the final decision on that which is considered offensive).*
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager.
- I will not allow unauthorised individuals to access personal details of any member of Eden Park High School.
- I will not download or install any software or resources from the Internet that can compromise data security, or are not adequately licensed by The Education for the 21st Century.
- I will not order, download or install any software without consulting the network manager.
- I will not order, download or install any software that can compromise data security, or is not licensed by the Education for the 21st Century.
- I understand that all Internet and network usage is monitored and logged, and this information could be made available to a line manager on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not knowingly connect a computer, laptop or other device (including USB flash drive), to the network which I know has software that can compromise the security of the school network.
- I will not use personal digital cameras or camera phones for the taking and/or transferring images of students or staff without written permission from a member of the Senior Leadership Team as well as the individual persons in the images.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused/associated with my professional role.
- I will not engage with any student or past student on a social networking site unless that site is approved by SLT.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Laptop loaned to you by the school must be brought into school at least once every 14 days for security updates and asset tracking.
- I will ensure any confidential data that I wish to transport from one location to another is protected by password or encryption and that I follow the school's data security protocols when using any such data at any location. If in doubt I will consult the network manager.

- I understand the data protection policy requires that any information seen by me with regard to staff or student information, held within the school's management information system (MIS), will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that all data held on school equipment is the property of the school and should need arise could be viewed at any time under the direction of the Headteacher.
- I will ensure I embed the school's safeguarding practice concerning e-safety within my classroom practice.
- I understand that providing students with any private telephone number or private e-mail addresses could lead to inappropriate use by others and that for this reason I will not give personal contact details to students.
- I will not allow any third party use of equipment, usernames, passwords issued to me. If this should happen I understand that I am accountable for the use that occurs in these circumstances. The only exception to this is theft or reported loss of equipment.
- I will abide by the schools password policy as defined by the network manager.
  The Current password policy is;
  - At least eight characters in length
  - Does not contain any part of your name and must contain characters from three of the following four categories;
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example,!, $, #, %) and I will change my password regularly
- I understand that failure to comply with this Acceptable Use Policy could lead to disciplinary action.

<u>User Signature</u>

- I understand that it is my responsibility to ensure that I remain up-to-date regarding e-safety safeguarding provision.
- I have read and understand the school's most recent Acceptable Use Policy, and agree to abide by it, and any reasonable revisions hereafter and which will be made public.
- I wish to have an email account, be connected to the Intranet and Internet, and be able to use the school's computer resources and systems.

Signature …… Date …… (dd/mm/yyyy)

Full Name …… (Please print)

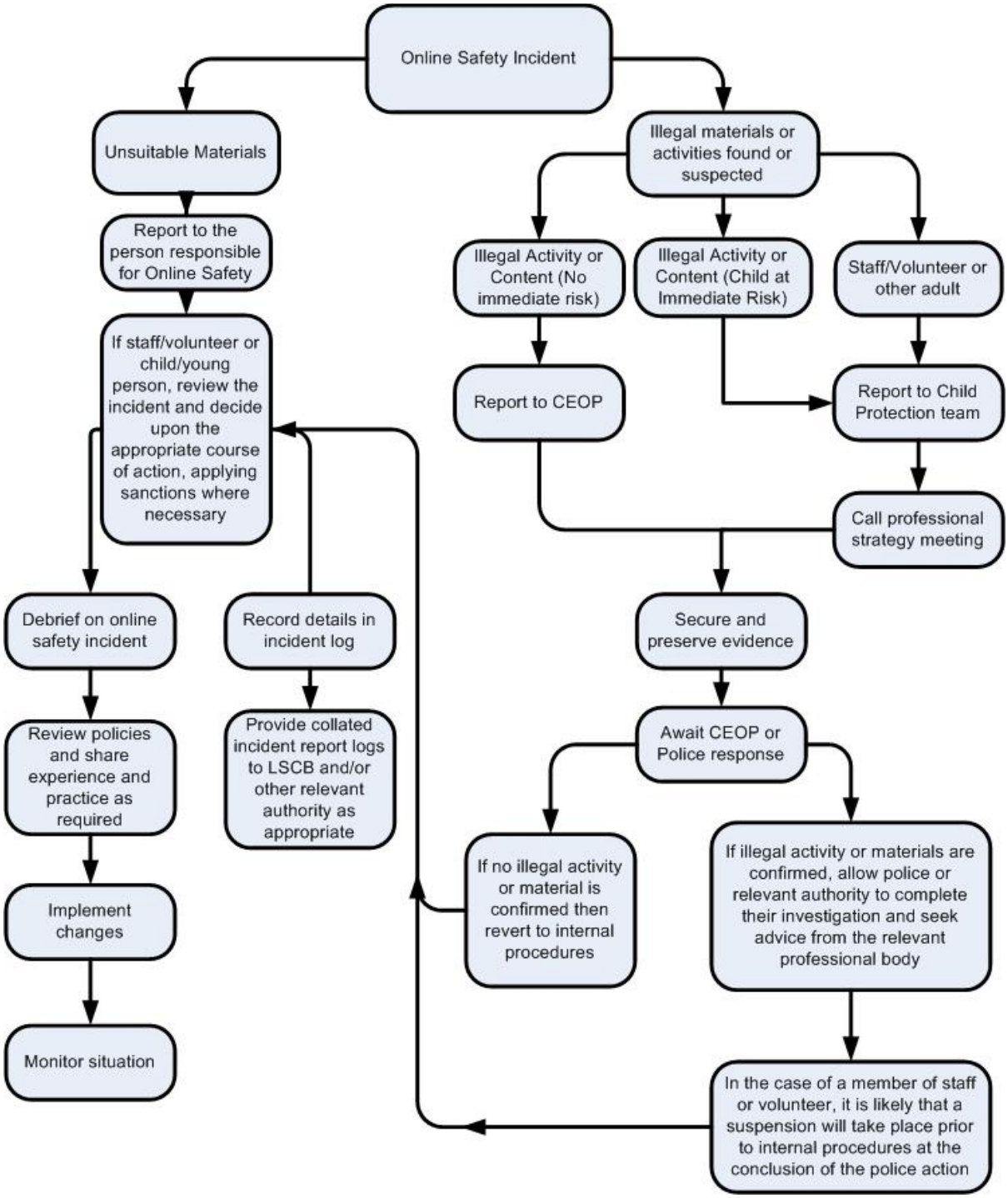
Job title ……

Authorising Signature: School's e-safety officer ◯ Network Manager ◯

I approve this user to have access to EPHS Digital Systems and Resources and to be set-up with a user account.

Signature …… Date ……

Responding to incidents of misuse – flow chart



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* infrastructure/network is as safe and secure as is reasonably possible and that:

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

Responsibilities

The management of technical security will be the responsibility of the lead IT Technician

Technical Security

Policy statements

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

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

- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager/Technical Staff (or other person) and will be reviewed, at least annually, by the Digital Citizenship Safety Group (or other group).
- 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 Lead 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 installations
- Mobile device security and management procedures are in place (Schools/ Academies may wish to add details of the mobile device security procedures that are in use).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view user activity.
- An appropriate system is in place for users to report any actual/potential technical incident to the Digital Citizenship Safety Coordinator/Network Manager/Technician (or other relevant person, as agreed).
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.
- An agreed policy 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 policy is in place 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 cannot 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 essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Digital Citizenship Safety Group (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master/administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by the designated IT technician. Any changes carried out must be notified to the manager of the password security policy (above).
- Users will change their passwords at regular intervals – as described in the staff and student sections below.
- Where passwords are set/changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a student)

Staff Passwords

- All staff users will be provided with a username and password by the lead IT technician who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- 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 six 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 180 days.
- should not re-used for 6 months and be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used.

Student Passwords

- All users will be provided with a username and password by the designated IT technician who will keep an up to date record of users and their usernames.
- Users will be required to change their password every 180 days.
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

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

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

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The lead IT technician will ensure that full records are kept of:

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

Filtering

Introduction

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

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the lead IT technician. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems. Eden Park High School currently uses Security.

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

- be logged in change control logs
- be reported to a second responsible person (the business manager):
- either be reported to and authorised by a second responsible person prior to changes being made
- be reported to the Digital Citizenship Safety Group as and when they are updated

All users have a responsibility to report immediately to an IT technician any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

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

- The school has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school 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 IT technician and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Digital Citizenship Safety Group.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the digital citizenship safety education programme. 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 policy through the Acceptable Use Agreement and through digital citizenship safety awareness sessions/newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT technician and Digital Citizenship Coordinator.

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 Digital citizenship Safety Policy 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:

- Safeguarding team and members of the pastoral team
- The second responsible person (**Business Manager**)
- Digital citizenship Safety Group
- Digital citizenship Safety Governor/Governors committee
- External Filtering provider/Local Authority/Police on request

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

School Personal Data Handling Policy Template

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 policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA defines "Personal Data" as data which relate to a living individual who can be identified
(http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- 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

Guidance for organisations processing personal data is available on the Information Commissioner's Office website:
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy 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".

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, 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 Business Manager. This person will keep up to date with current legislation and guidance and will:

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

The school will identify Information Asset Owners (IAOs) 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 policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. (each school is responsible for their own registration): http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DfES, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers through the information pack. Parents/carers of young people who are new to the school will be provided with the privacy notice through their information pack.

Training & awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- 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;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

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 RESTRICT.

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.

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.

Secure Storage of and access to data

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

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

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

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.
The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, 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.

As a Data Controller, the school 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 school 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
- 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.

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, and other media must be shredded, incinerated or otherwise disintegrated for data.

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.

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 policy, for example.

The school has a policy 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 policy and communication plan.

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 digital citizenship and telephone support, service guarantees

Audit / Monitoring / Reporting / Review

The responsible person *(Digital Citizenship Coordinator)* 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 Digital Citizenship Coordinator/Digital citizenship Safety Committee/Digital citizenship Safety Governor at regular intervals (**annually**)

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

School Policy Template – Digital citizenship Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from Eden Park High School community, with responsibility for issues regarding digital citizenship safety and the monitoring the digital citizenship safety policy including the impact of initiatives.

2. Membership

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

The composition of the group will include

- Pastoral Board
- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Digital citizenship safety coordinator
- Governor
- Parent / Carer
- IT Technical Support staff (where possible)
- Student representation – for advice and feedback. Student voice is essential in the make-up of the digital citizenship safety group, but students would only be expected to take part in committee meetings where deemed relevant.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

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

2.4. Committee 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. Chairperson

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

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

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

5. Functions

Functions of the Digital Citizenship Safety Coordinator include the following any other determined by the headteacher as deemed necessary:

- To keep up to date with new developments in the area of digital citizenship safety
- To (at least) annually review and develop the digital citizenship safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the digital citizenship safety policy
- To monitor the log of reported digital citizenship 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 digital citizenship 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
  - Digital citizenship 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

6. Amendments

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

The above Terms of Reference for the Education for the 21st Century – Eden Park High School have been agreed

Signed by (Headteacher/SLT): ----------

Date: ----------

Date for review: ----------

Legislation

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

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.)

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-digital_citizenship
Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Glossary of Terms

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

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