E-Safety Policy

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.
Tel. 0844 800 2382 **Email** esafety@swgfl.org.uk **Website** www.swgfl.org.uk

SWGfL Online Safety School Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by:

- Headteacher
- Computing Curriculum Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors

This e-safety policy will continue to be developed and reviewed with regular feedback and communications with Parents, Carers and Community users.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	*Due to be ratified on 13.07.20*
The implementation of this e-safety policy will be monitored by the:	Computing Curriculum Lead SLT Governors
Monitoring will take place at regular intervals:	December – annually
The Governing Board will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually in December, following the monitoring Any safeguarding incidents that should be reported to Governors will be included in the termly Safeguarding Report
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	June 2021 for ratification by FGB in July 2021
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Head Teacher, Safeguarding Governor, LADO, ICT management company, SWLG, RMUnIfy, Police – depending on the circumstances

The school will monitor the impact of the policy using:

- CPOMs reported incidents by teaching staff
- Monitoring logs of internet activity (including sites visited) checking history registers on hardware
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

SWGfL Online Safety School Policy

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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 e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Board receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor, this includes e-safety. The role of the E-Safety/Safeguarding Governor will include:

- regular contact with the Computing Curriculum Lead and/or Head Teacher
- regular monitoring of e-safety incident log analysis
- regular monitoring of SWLG and RMUnify filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Curriculum Lead.
- 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 e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Computing Curriculum Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The annual monitoring will be undertaken by the Computing Curriculum Lead with a member of the Senior Leadership Team.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Curriculum Lead.

Computing Curriculum Lead:

The Computing Curriculum Lead:

- leads the e-safety teaching, learning and assessment.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the

school e-safety policy.

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority for communications, networking and training events, as well as Safeguarding information.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- communicates regularly with Head Teacher and/or E-Safety/Safeguarding Governor to discuss current issues.
- attends a relevant Full Governing Board meeting when requested to present relevant information.
- reports regularly to Senior Leadership Team.

The Computing Curriculum Lead will:

- produce / review / monitor the school e-safety policy / documents.
- produce / review / monitor the school filtering procedures and requests for filtering changes.
- map and review the e-safety curricular provision – ensuring relevance, breadth and progression
- monitor network / internet / incident logs
- consult stakeholders – including parents / carers and the pupils / pupils about the e-safety provision
- monitor improvement actions identified through use of the 360 degree safe self review tool

Network Manager / Technical staff:

The Computing Curriculum Lead, along with the Headteacher, is responsible for confirming that, the provider of the managed ICT service, ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- filtering is regularly updated by our internet provider, email system provider and the ICT service provider.
- that they are fully aware of the school e-safety policy and procedures.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network, internet, remote access and email are regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Computing Curriculum Lead for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher or Computing Curriculum Lead for investigation.
- all digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.

- pupils understand and follow the e-safety and acceptable use policies.
- pupils 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils:

Pupils must ensure that they:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-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 and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about local and national e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to sections of the website.
- their children's personal devices in the school.

Community Users

Community Users who access school systems and website as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – pupils

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

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

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the Pupil 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg 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 e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and 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.
- Letters, newsletters, website.
- Parents evenings and events.
- High profile events e.g. Safer Internet Day
- Reference to the relevant websites on the Safeguarding documents and Online Safety page
  https://hesterswayprimaryschool.co.uk/home-learning/#OnlineSafety
  www.swgfl.org.uk
  www.saferinternet.org.uk/
  http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community.

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process. At present, this involves all staff completing the online e-safety CPD course at: https://www.onlinesafetyalliance.org/cpd-2020/
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy. New staff will be expected to work through the staff training as outlined above.
- E-safety sessions will be delivered to children and staff together by the local PCSO annually, which will provide regular updates to the training.
- The Computing Curriculum Lead will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings or INSET days.
- The Computing Curriculum Lead will provide advice, guidance and training to individuals as required.

Training – Safeguarding Governor

The Safeguarding Governor should take part in e-safety training and awareness sessions, and other Governors be aware of e-safety through e-safety awareness sessions and Child Protection training.

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (eg SWGfL).
- Participation in school training or information sessions for staff or parents.
- Completion of the online training at: https://www.onlinesafetyalliance.org/cpd-2020/

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-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 academy 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 adult users will be provided with a username and secure password by Focus Networks (on the direction of the Headteacher) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Users should be aware that changing passwords regularly is good practice. Pupils will have class log-on details.

- The administrator passwords for the school ICT system, used by Focus Networks must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- *The Finance Officer* 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
- Staff will report any need to adapt and change the filter for specific site to the Computing Curriculum Lead who will report it to SWLG
- 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.
- Approved visitors to the site will get a copy of the AUP policy and school password for the WIFI
- Supply teachers will sign in as a guest – Computing Lead to liaise with our IT company on the number and allocation of guest log ins
- School computers and Ipads are for school use only at home due to GDPR and confidential information held on them. Personal phones are not permitted on the school WIFI staff and visitors should use their own data allowance.
- As our IT company installs log ins they are in control of programmes put onto laptops and Ipads (push out from software). No staff have admin privileges. The IT company remotes into computers and laptops to fix any issues.
- Removable media should have passwords to protect information. The IT company is asked to encrypt laptops to protect information. Personal information regarding pupils should be sent to external agencies vis the Egress email system which staff can create free accounts. CPOMs is used to communication incidents, first aid and other safeguarding information. When emailing about pupils initials should be used rather thatn the child's name. It is better to have internal phone calls when others are no privy to the information for confidential information sharing.
- Staff must remember that under GDPR that when a Subject Access Request (SAR) is made the persons initials, name and details can be searched for under all school systems. Staff must write factual statements at all times.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. At present, we do not permit users to bring their own devices into school and personal devices should not be connected to the school network.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in

not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital images or videos.

- Staff and volunteers are allowed to take digital images and videos 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 images and videos that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers and should not include the full name of the pupil.

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.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed to keep records of assets.
- 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 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 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:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		✓*				✓*		
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices	✓**						✓**	
Use of personal email addresses in school should be on a personal devices during break time and not on the school network	✓							✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media			✓					✓
Use of blogs	✓							✓

*: Pupils must put give their phones to their teacher who will lock it away, turned off, through the school day. Staff must keep their phones, turned off, in a locked cupboard, except at break times, when no pupils are present. Staff must ask the Head Teacher if they can turn their phone on in the cupboard, in emergency situations.

**: School iPads only

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

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, 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.
- Pupils will not be provided with school email addresses.
- Pupils should be taught about e-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 pupils and staff. Schools 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 liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: 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 pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Computing Curriculum Lead and/or Head Teacher to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

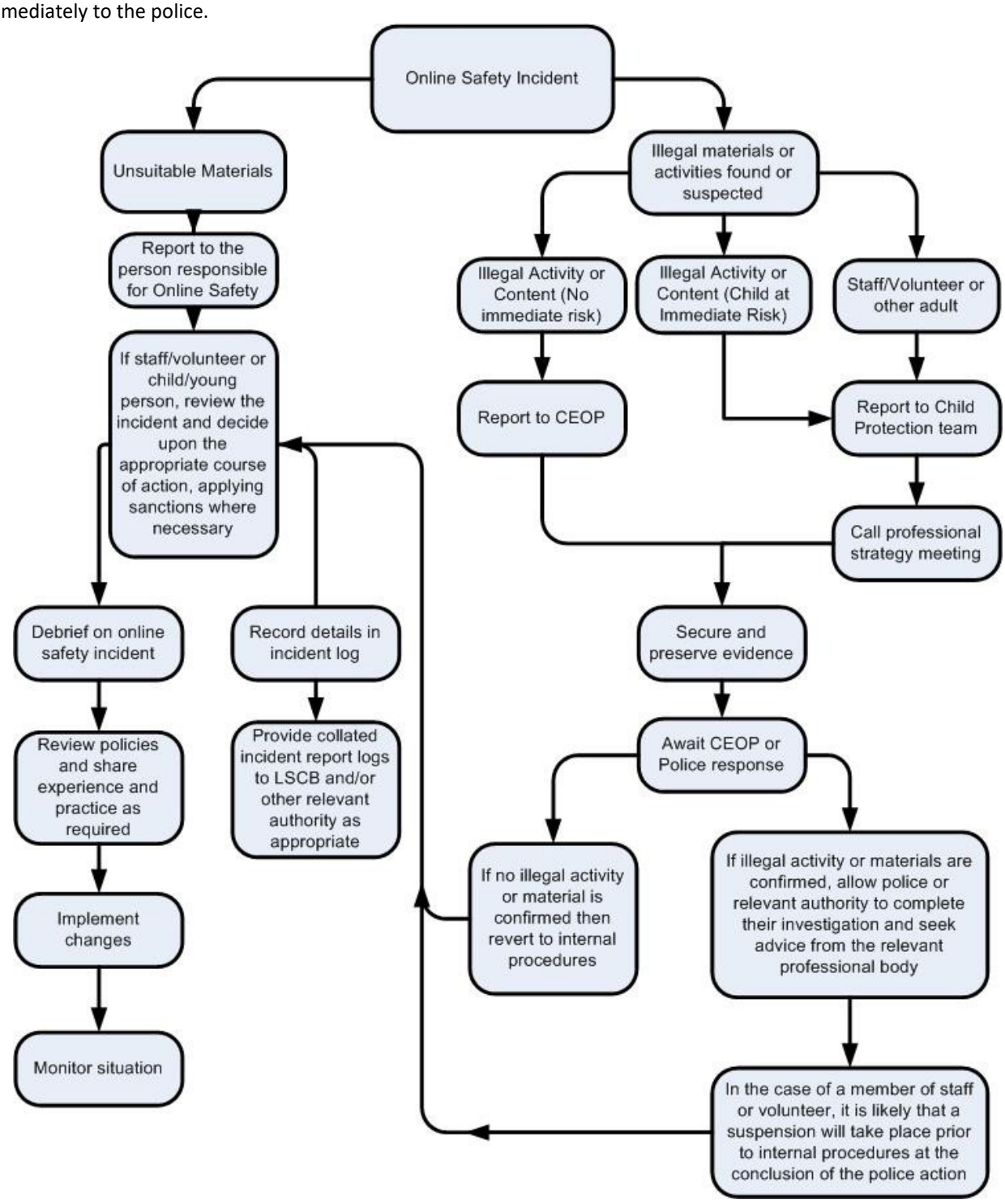
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce (items for school use only, with prior agreement of Headteacher)			X			
File sharing (via school network only, including remote access)		X				
Use of social media				X		
Use of messaging apps					X	
Use of video broadcasting e.g. Youtube – Kids Youtube preferred (Viewing only – uploading not permitted)		X				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority 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
    - 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 child protection 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 disciplinary procedures as follows:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X						X	
Unauthorised use of social media / messaging apps / personal email	X				X		X	
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords		X			X	X		
Attempting to access or accessing the school / academy network, using the account of a member of staff		X			X	X		
Corrupting or destroying the data of other users							X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			
Continued infringements of the above, following previous warnings or sanctions		X			X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		
Using proxy sites or other means to subvert the school's / academy's filtering system		X		X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X			

Staff Actions / Sanctions

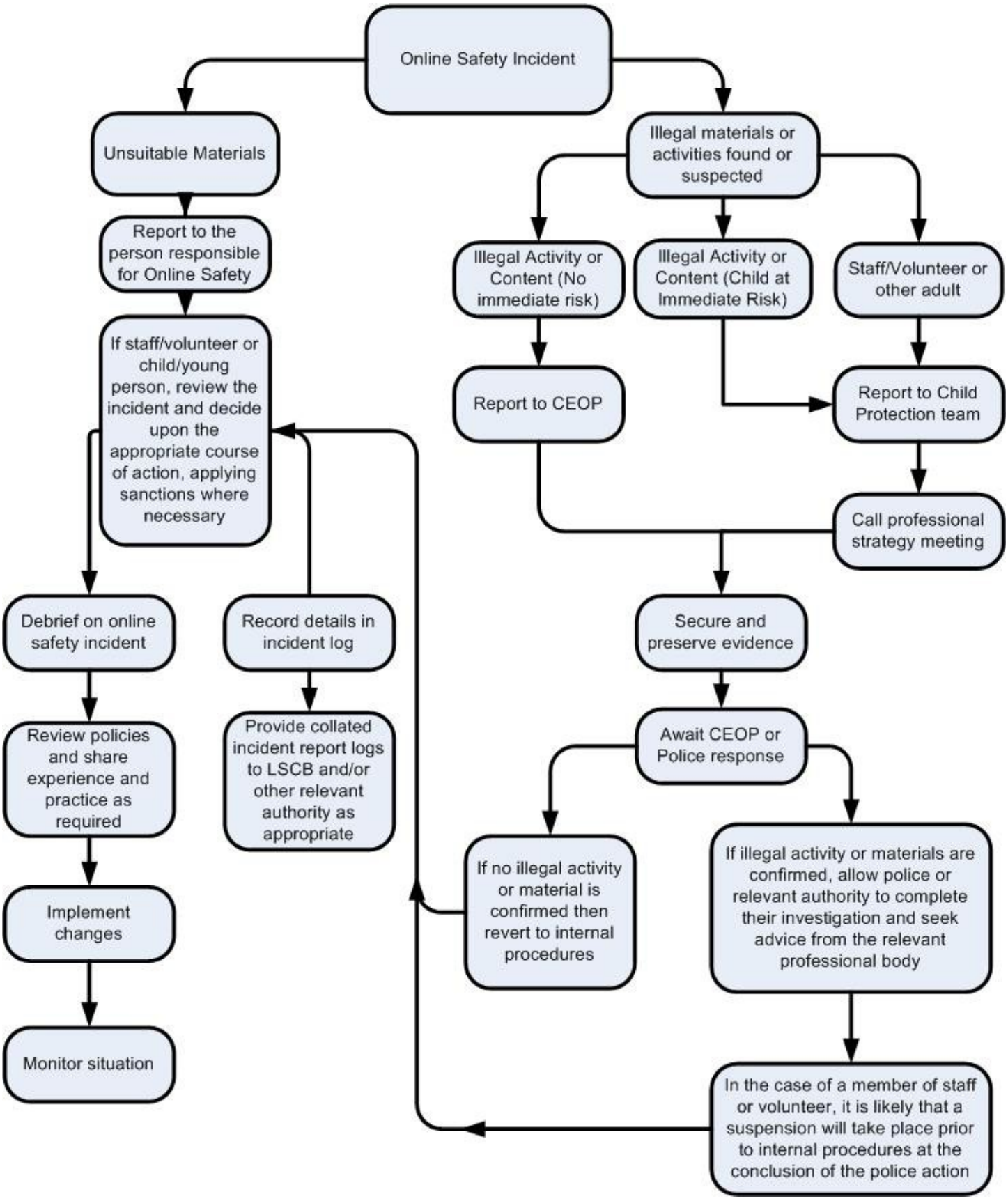
Incidents:	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable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

Acknowledgements

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

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

Responding to incidents of misuse – flow chart



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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Template Reporting Log

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

Training Needs Audit

Training Needs Audit Log

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

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

School Technical Security Policy (including filtering and passwords) – July 2020

Introduction

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

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

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that might otherwise be carried out by the school. It is also important that the managed service provider is fully aware of the school E-Safety Policy / Acceptable Use Agreements). The school should also check their Local Authority / other relevant body policies / guidance on these technical issues.

Responsibilities

The management of technical security will be the responsibility of the Computing Curriculum Lead in conjunction with the Headteacher and IT Service Provider.

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 will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined access rights to school technical systems.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Finance Officer/IT Service Provider are 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 devices should not be connected to the school network.
- 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 or potential technical incident to the Computing Curriculum Lead. Forms are provided in an Appendix to the E-safety Policy.
- An agreed statement and agreement is in place for the provision of temporary access of "guests", as part of the Safeguarding procedures, for visitors who need internet access. Permission will only be given by the Head Teacher.
- The IT service provider installs programmes on school devices. Users should not download executable programmes or install software. If software is to be installed, this will be done by the service provider.
- Staff should use their work laptop for work only and their family members are not allowed on school devices that may be used out of school. This is for data protection and safeguarding reasons. See the E-Safety Policy for details.
- Removable media (e.g. memory sticks / CDs / DVDs) should be encrypted/password protected. See the E-Safety Policy for details.
- 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 and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The administrator passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Provider or admin of the system.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described below
- Requests for password changes should be authenticated by the Headteacher to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password by the Head Teacher for emails and Insight Tracking; CPOMs the DHT; Network – IT provider.
- the password should be a minimum of 8 characters long and should 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 6 months.
- should not re-used for 6 months and be significantly different from previous passwords created by the same user.

Student / pupil passwords

Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class log-ons for KS1 (though increasingly children are using their own passwords to access programmes). *Schools* need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network / internet access. Schools should also consider the implications of using whole class log-ons when providing access to learning environments and applications, which may be used outside school.

- All pupils will be provided with a username by the IT provider.
- Users will be required to change their password every year.
- Students / pupils will be taught the importance of password security.
- The complexity (ie 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 e-safety policy.
- through the Acceptable Use Agreement.

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

- in lessons.
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person Computing Lead/Head teacher/IT provider will ensure that full records are kept of:

- User Ids and requests for password changes.
- User log-ons.
- 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 e-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.

We are aware of the flexibility provided by many filtering services at a local level for school. Where available, we will use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

We will:

- use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users.
- Computing Lead and Head Teacher to agree the filtering procedures and decisions.
- the IT provider will recommend up to date filtering and software to safeguard the IT in school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Computing Curriculum Lead. They will manage the school filtering, in line with this policy and will keep records of changes and of breaches of the filtering systems.

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

- be logged in change control logs.
- be reported to a second responsible person, namely the Headteacher prior to changes being made.

All users have a responsibility to report immediately to the Computing Curriculum Lead 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. Illegal content is filtered by broadband/firewall 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 maintains and supports the managed filtering service provided by the Internet Service Provider.
- The school has provided enhanced / differentiated user-level filtering through the use of the SWLG filtering programme.
- 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.
- 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 Computing Curriculum Lead with the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Computing Curriculum Lead.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-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 e-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 Computing Curriculum Lead or the Headteacher who will decide together whether to make school level changes (as above).

If a staff user wishes to request a change to the filtering, the request should be made in writing to the Computing Curriculum Lead or Headteacher, explaining what change they would like, the reason for the change and the duration of the change. Changes will only be permitted if there are strong educational reasons. Any changes will be monitored closely.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows: the Computing Lead and Head Teacher will check school devices termly to ensure they ar being used correctly and the policies are followed.

Audit / Reporting

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

- the Senior Leadership Team
- E-Safety/Safeguarding Governor
- External Filtering provider / Local Authority / Police on request

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

Further Guidance

Schools / academies may wish to seek further guidance. The following is recommended:

NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html

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

School Policy Template: Electronic Devices - Searching & Deletion – July 2020

Introduction

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

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

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

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

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

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

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

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

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Relevant legislation:

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

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

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

This policy has been written by and will be reviewed by: the Headteacher, the Board of Governors and the Computing Curriculum Lead.

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

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training. Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training / Awareness

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

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

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

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

Policy Statements

Search:

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

Pupils are only allowed to bring mobile phones or other personal electronic devices to school if they hand them in to the teacher at the start of the day, to be returned at hometime. It is forbidden for pupils to use them in the school.

If pupils breach these roles, the sanctions for breaking these rules can be found in the Behaviour Policy

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

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

In carrying out the search:

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

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

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

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

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

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

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

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

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

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

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

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

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

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

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

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

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

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

Care of Confiscated Devices

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

Audit / Monitoring / Reporting / Review

The Headteacher 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 E-Safety Governor at regular intervals.

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.

Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 1998

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

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

Freedom of Information Act 2000

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

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harrassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

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:
http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Links to other organisations or documents

The following links may help those who are developing or reviewing a school E-safety policy.

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/

ThinkUKnow

Others:

INSAFE http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

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

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

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

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

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

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

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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 e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

Pupils are taught:

Safe surfing

Surfing the Net can be great fun, but here are some easy rules to remember that will keep you safe while you surf:

Don't give out your personal information - Don't put personal details such as your home address, telephone numbers, email address, school name

What goes online, stays online - Use privacy settings to make sure only your friends and family can see photos you post

Check your security and privacy settings - Make sure your social network privacy settings are secured so only your friends can see your personal information and use your privacy settings to restrict who can see your posts, videos and photos

Password safety - Keep your Internet passwords private and change them often. Use a hard to guess password with both CAPITAL and small letters, numbers and other symbols such as: @ # ,. &.

Don't talk to strangers online- Only talk to people you actually know. Do not become friends with strangers online. Be careful making friends with people who claim to know your friends - check that somebody else knows them well before adding them to your social network.

Never agree to meet someone that you have met on the Internet.

Be wary of unsecured or unknown websites - When shopping online, use reputable and known retailers, make sure any transactions you make only take place across secure web pages which you can identify from the padlock sign in your browser address bar and where the address says https.

Use bookmarks to access your favourite websites and, if you know the web address, type it into the box at the top of the page rather than using a search engine such as Google or Yahoo. When searching for a site on Google take time to look at the website results. The first site that comes up may not be the site you are looking for. Some websites may not be genuine but may have a very similar address.

Be careful what links you click on - Avoid clicking links in an email, instant message or on your social network unless you are sure the message is from someone you know.

If you enter a site or receive information that makes you feel uncomfortable, tell someone you trust.

Always protect your mobile device - Make sure your mobile phone is pin-protected so all your personal information stored on it is safe. Download a security app which allows you to remotely wipe any personal data, should your mobile be lost or stolen

Strangers online - Learn some common tricks of online predators

Only talk to people you actually know. Do not become friends with strangers online. Be careful making friends with people who claim to know your friends - check that somebody else knows them well before adding them to your social network.

Stay 'SMART'

Safe - Keep safe by being careful not to give out personal information such as your name, email, phone number, home address, or school name - to people who you don't know or trust online.

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents or carers' permission and even then only when they can be present.

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.

Reliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at Think you know.

At School: Internet Rules

These are the rules we follow to keep us all safer on the internet when we are learning.

- ✓ **Log on with your own password**, or one that the teacher has given you.
- ✓ **Make sure** that you never give your own or anyone's details over the Internet. This includes full name, address, telephone number, email address, mobile number or photograph.
- ✓ **Make sure** that you never give the school's name unless you have permission from your teacher.
- ✓ **Never agree** to meet anyone who contacts you on the internet. Always tell your teacher if someone asks you to do this.
- ✓ **Always tell your teacher** if you see anything, which makes you feel uncomfortable. Switch off the monitor.
- ✓ **Always tell your teacher** if someone sends you a nasty message. Remember it is not your fault if you get a message like this.
- ✓ **Make sure** you only go on websites your teacher gives you permission to use.
- ✓ **Only** go on the Internet when your teacher is in the room.
- ✓ **Never download** music or programs without permission.
- ✓ **Remember** that the school may check your computer files and may look at the internet sites that you visit.