

Contents

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities

- Governors
- Headteacher / Principal and Senior Leaders
- E-Safety Co-ordinator / Officer
- Network Manager / Technical Staff
- Teaching and Support Staff
- Child Protection / Safeguarding Designated Person / Officer
- E-Safety Committee
- Students / Pupils
- Parents / Carers
- Community Users

Policy Statements

- Education – Students / Pupils
- Education – Parents / Carers
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Bring your own devices (BYOD)
- Use of digital and video images
- Data protection
- Communications
- Social Media - Protecting Professional Identity
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse

E-Safety Policy: KSSS

OFSTED: IMMEDIATE MONITORING.

PCE weekly monitoring reports

AUP

Stepping Forward Together – Caring, Sharing & Aspiring

Development / Monitoring / Review of this Policy:

This e-safety policy has been developed by a working group of staff made up of:

- *Headteacher: K. Rogers*
- *E-Safety Coordinator: N Best*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Management Committee*
- *Parents and Carers*
- *Community users*

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the <i>Management Committee</i> :	<i>FEB 2015</i>
The implementation of this e-safety policy will be monitored by the:	<i>Headteacher; Esafety Coordinator; SLT & MC</i>
Monitoring will take place at regular intervals:	<i>least once a year: Dec/Jan time</i>
The <i>Management Committee</i> 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:	<i>least once a year: Feb</i>
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:	<i>Least once a year: Oct/Nov</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>Headteacher: K Rogers LA – Inclusion Officer: A Greenwood / L Mitchell LA Safeguarding Officer Police</i>

The school will monitor the impact of the policy using:

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

- *staff*

Scope of the Policy:

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

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 KSSS 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 KSSS but is linked to membership of the KSSS. 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.

KSSS 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 KSSS.

Governors of Management Committee: R. Randle

Governors of the Management Committee 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 *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Management Committee* has taken on the role of *E-Safety Governor* ROZ RANDLE can combine e-safety with that of the Child Protection / Safeguarding Governor). The role of the *E-Safety Governor* will include:

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors Management Committee – T&L*

Headteacher, K Rogers and Senior Leadership Team L Georgiou; F Perry & L Bailey:

- **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 *E-Safety Co-ordinator*.
- **The Headteacher and Deputy Headteacher are 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 / other relevant body* disciplinary procedures). SWGfL BOOST includes an 'Incident Response Tool' that steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. This can be downloaded at <http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool>

- *The Headteacher & Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. SWGfL BOOST includes access to unlimited online webinar training – further details are at <http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>*
- • *The Headteacher & Senior Leadership Team 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 E-safety Coordinator will receive regular updates through attendance at LA / training sessions and by reviewing guidance documents released by LA and others. The E-safety Coordinator will also provide advice, guidance and training as required to individuals as required.*
- *The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.*

E-Safety Coordinator: N Best

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- 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 / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets may be found later in this document). SWGfL BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper>)
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of *Governors of the Management Committee*
- reports regularly to Senior Leadership Team
- ensures that policy is consistent and complies with the **Computer Misuse Act 1990** and the **Data Protection Act 1998**
- Ensures that internal and external communications are compliant with the **Malicious Communications Act 1988**
- Assists the Headteacher in regulating the behaviour of students in accordance with the **Education and Inspections Act 2006**

Network Manager & Technical staff: N Best with J Highfield

(nb. if the *school / academy* has a managed ICT service provided by an outside contractor, it is the responsibility of the *school / academy* to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the *school / academy* e-safety policy and procedures.)

The *Network Manager & Technical Staff* responsible for ensuring:

- that the *school's / academy's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school / academy* meets required e-safety technical requirements and any *Local Authority / other relevant body* E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher & E-Safety Coordinator & Technical Staff* for investigation; action & sanction to be carried out by the Headteacher
- that monitoring software / systems are implemented and updated as agreed in KSSS policies

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of KSSS e-safety policy and practices
- they have read, understood and signed the digital Staff Acceptable Use Policy / Agreement (AUP). The policy is displayed and affirmed as part of accessing the intranet.
- they report any suspected misuse or problem to the *Headteacher & E-Safety Coordinator* for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person: K Rogers & L Georgiou

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

(nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Some schools may choose to combine the role of Child Protection Officer / Safeguarding Officer and E-Safety Officer)

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the *school / academy* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the *school / academy* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body / Directors*.

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Coordinator / Officer* (or other relevant person, as above) with:

- the production / review / monitoring of the school e-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 e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

(Schools / academies will need to decide the membership of the e-safety group. It is recommended that the group should include representation from students / pupils and parents / carers).

An E-Safety Group Terms of Reference Template can be found in the appendices

Students / pupils:

- **are responsible for using KSSS 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 KSSS 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 / mobile devices in an appropriate way. KSSS will take every opportunity to help parents understand these issues through *PRDs, letters, website and information about national / local e-safety campaigns / literature*. Parents and carers will be encouraged to support KSSS in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in KSSS (where this is allowed)

Community Users: KSSS has none except authorised visitors

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 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 IS provided as part of Creative Media, PHSE and other lessons (as and when students need to be reminded).**
- **Key e-safety messages ARE reinforced as part of a programme of assemblies and tutorial / pastoral activities**
- **Students ARE 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 ARE taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *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 (eg racism, drugs, discrimination etc) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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 / regulation of the children's on-line behaviours. Parents/ carers 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:

- *Pre – Admissions meetings and the Student Induction Pack*
- *Letters, web site,*
- *PRDs*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> (see appendix for further links / resources)*

Education – The Wider Community: at KSSS copies in main office and taken to N Best

It is essential that visiting agencies and staff are aware of the obligations and parameters required when using the schools network. As such they will be required to sign and accept a visitors ICT Acceptable Use Agreement.

In signing I accept the conditions set out below and agree to abide by the school's E-safety policy.

- I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner and that the ICT and related systems are school property.
 - I will ensure that my information systems * use is restricted to that necessary to achieve the agreed purpose of my visit.
 - I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
 - I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
 - I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
 - I will not install any software or hardware without permission.
 - I will respect copyright and intellectual property rights.
 - I will report any incidents of concern regarding inappropriate use to the headteacher.
 - The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- * Information systems includes telephone, fax etc.

Name:

Signed:

Date:

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.** SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>) *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff WILL receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.** SWGfL BOOST includes an array of presentations and resources that can be presented to new staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources>)
- *The E-Safety Coordinator & or Headteacher will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.* SWGfL BOOST includes an array of presentation resources that the e-Safety coordinator can access to deliver to staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources>). It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors of Management Committee:

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members involved in health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring:

If the school / academy 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 would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of KSSS E-Safety Policy & Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues. KSSS use LA Staff and equipment.

KSSS IS 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 e-safety responsibilities:

- **KSSS technical systems will be managed in ways that ensure that KSSS meets recommended technical requirements** (these may be outlined in Local Authority / other relevant body policy and guidance)

- **There will be regular reviews and audits of the safety and security of KSSS 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 / academy technical systems and devices.**
- **All users will be provided with a username and secure password by *(the Network Manager)* who keeps 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 periodically.**
- **The “master / administrator” passwords for KSSS ICT system, used by the Network Manager (or J Highfield) must also be available to the *Headteacher* and kept in a secure place (eg school safe)**
- **The [Network Manager](#) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by Staffordshire Learning Technologies through 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. [Direct contact is required, through the Network Manager or Headteacher to SLT \(Staffordshire Learning Technologies\).](#)
- [KSSS has provided enhanced / differentiated user-level filtering \(allowing different filtering levels for different ages / stages and different groups of users – System Administrators /staff / pupils / students etc\)](#)
- [KSSS technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.](#)
- [An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. Any report should first be made to the Network Manager or Associate Technician. If the report concerns the Network Manager or Associate Technician then it should be referred to the Headteacher.](#)
- [Appropriate security measures are in place \(provided through Symantec\) 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, as described in the visitor AUP above, for the provision of temporary access of “guests” \(eg trainee teachers, supply teachers, visitors\) onto the school systems.](#)
- [An agreed policy is in place, as described in the AUP and induction procedure, regarding the extent of personal use that users \(staff / students / pupils / community users\) and their family members are allowed on school devices that may be used out of school.](#)
- [An agreed policy is in place, as described in the staff handbook and digital AUP, that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.](#)
- [An agreed policy is in place, as described in the 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. \(see \[School Personal Data Policy Template\]\(#\) in the appendix for further detail\)](#)

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. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies. ([see appendix for a more detailed BYOD Policy Template](#))

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

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. KSSS 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 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 is 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. [Refer to SCC document re use of multi media & DfE document Guidance for working practice for adults who work with children & YP in education settings.]*
- *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.*

- *Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)*
- *Student's / Pupil's work can only be published with the permission of the student / pupil 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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to this document. (Schools / Academies should review and amend this appendix, if they wish to adopt it. Schools / Academies should also ensure that they take account of relevant policies and guidance provided by local authorities or other relevant bodies).

KSSS will 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". (see Privacy Notice section in the appendix)**
- **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 - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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 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 (many memory sticks / cards and other mobile devices cannot 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 will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.)

The Personal Data Handling Policy Template in the appendix provides more detailed guidance on the school's / academy's responsibilities and on good practice.

Communications:

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow students / pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students / pupils. The table has been left blank for school to choose its own responses.

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				
	Allowed	Allowed at certain times	Allowed for selected staff	NOTES	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	Y				Y			
Use of mobile phones in lessons		Y		1:1 basis				N
Use of mobile phones in social time	Y							N
Taking photos on mobile phones / cameras	N							N
Use of other mobile devices eg tablets, gaming devices	N							N
Use of personal email addresses in school, or on school network		Y						N
Use of school email for personal emails	N							N
Use of messaging apps	N							N
Use of social media	N							N
Use of blogs	N							N

When using communication technologies KSSS considers the following as good practice:

- **KSSS 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 KSSS email service to communicate with others when in school, or on KSSS systems (eg by remote access).
- **Users must immediately report, to the HEADTEACHER – in accordance with KSSS 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.** (SWGfL BOOST includes an anonymous reporting app Whisper - <http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper>)
- **Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) KSSS systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students 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 KSSS website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils 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 KSSS & 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. SWGfL BOOST includes unlimited webinar training on this subject: (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>)
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

KSSS staff should ensure that:

- No reference should be made in social media to students, 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 KSSS or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

KSSS's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies. SWGfL BOOST includes SWGfL Alerts that highlight any reference to the school/academy in any online media (newspaper or social media) for example <http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Alerts>

Unsuitable / inappropriate activities:

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities eg 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.

KSSS 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		X				
File sharing				X		
Use of social media		X				
Use of messaging apps			X			
Use of video broadcasting eg Youtube			X			

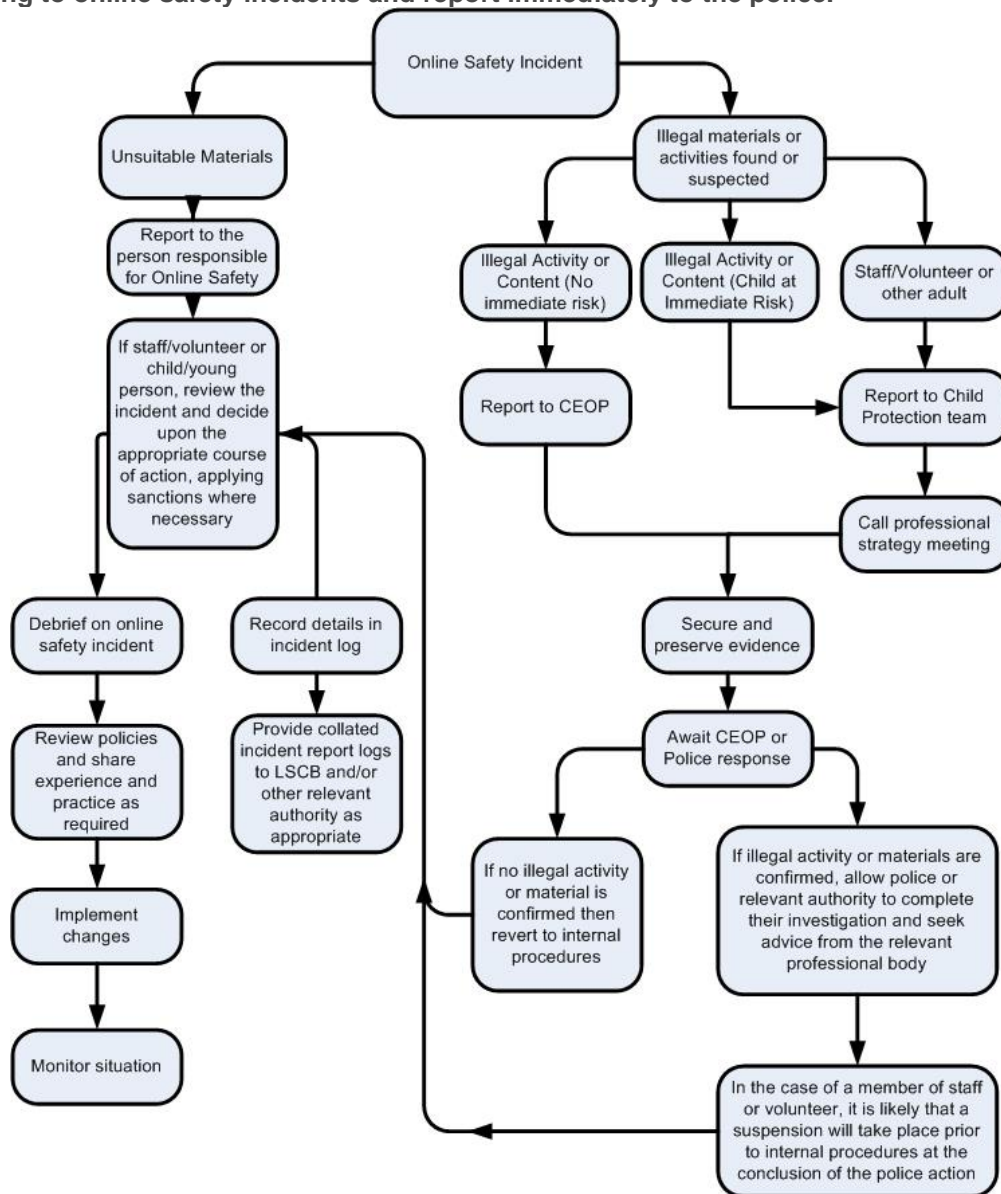
Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above). [SWGfL BOOST includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when](#)

managing reported incidents (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool>)

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 KSSS 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 / 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
 - 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 KSSS 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.

KSSS Actions & Sanctions:

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

Students / Pupils

Actions / Sanctions

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

Staff

Actions / Sanctions

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

Appendix

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

<http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy>

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

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2013. However, SWGfL can not guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2013

Appendices

Can be found on the following pages:

• Student / Pupil Acceptable Use Agreement template (older children)	25
• Student / Pupil Acceptable Use Agreement template (younger children)	29
• Parents / Carers Acceptable Use Agreement template	30
• Staff and Volunteers Acceptable Use Agreement Policy template	34
• Community Users Acceptable Use Agreement	37
• Responding to incidents of misuse – flowchart	38
• Record of reviewing sites (for internet misuse)	39
• School Reporting Log template	40
• School Training Needs Audit template	41
• School Technical Security Policy template	42
• School Personal Data Policy template	49
• School Policy Template – Electronic Devices, Search and Deletion	61
• School Bring Your Own Devices (BYOD) Template Policy	67
• School E-Safety Committee Terms of Reference	68
• Legislation	70
• Links to other organisations and documents	73
• Glossary of terms	76

Student / Pupil Acceptable Use Agreement Template – for older students / pupils

Sections that include advice or guidance are written in **BLUE**. It is anticipated that schools will remove these sections from their final AUP document. Schools should review and amend the contents of this AUA to ensure that it is consistent with their E-Safety Policy and other relevant school policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AU Agreement will be more concise.

School / Academy Policy

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy Agreement

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

For my own personal safety:

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

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

- I understand that the *school / academy* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school / academy* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so. (*schools / academies* should amend this section to take account of their policy on each of these issues)

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

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

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

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission (*schools / academies should amend this section in the light of their mobile devices policies*). I understand that, if I do use my own devices in the school / academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed (*schools / academies should amend this section to take account of their policy on access to social media*).

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

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

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

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

Student / Pupil Acceptable Use Agreement Form

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

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems. (Schools / academies will need to decide if they require students / pupils to sign, or whether they wish to simply make them aware through education programmes / awareness raising).

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

- I use the *school / academy* systems and devices (both in and out of school)
- I use my own devices in the *school / academy* (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the *school / academy* in a way that is related to me being a member of this *school / academy* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature (optional)

It is for schools / academies to decide whether or not they require parents / carers to sign the Parent / Carer Acceptable Use Agreement (see template later in this document). This includes a number of other permission forms (including digital and video images / biometric permission / cloud computing permission).

Some schools / academies may, instead, wish to add a countersignature box for parents / carers to this student / pupil Acceptable Use Agreement.

Student / Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):.....

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent):

This AUP is based on one produced by St Mark's Church of England / Methodist Ecumenical VA Primary School, Weston super Mare.

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the Parent / Carer Acceptable Use Agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

Parent / Carer Acceptable Use Agreement Template

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

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work. (Schools / academies will need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

Permission Form

Parent / Carers Name Student / Pupil Name

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

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s / daughter’s activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.

Signed Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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 / pupils* in the digital / video images.

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

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent' for their children to be able to use these services. It is suggested that schools will incorporate this into their standard acceptable use consent forms sent to parents each year.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses Google Apps for Education for *pupils / students* and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each *pupil / student* and hosted by Google as part of the school's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, *pupils / students* collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

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

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to my child using the school using Google Apps for Education.

Yes / No

Signed

Date

Use of Biometric Systems

If the school uses biometric systems (eg fingerprint / palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" legislation) seek permission from a parent or carer. It is also recommended that they obtain this permission through the normal internet use permission / acceptable use agreement. Schools may therefore wish to add a section such as that below to this permission form.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole **fingerprint / palm print** of my child and that these images will not be shared with anyone outside the school.

Yes / No

Signed

Date

Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

It is suggested that when the Student / Pupil AUP is written that a copy should be attached to the Parents / Carers AUP Agreement to provide information for parents and carers about the rules and behaviours that students / pupils have committed to by signing the form.

Staff (and Volunteer) Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in **BLUE**. It is anticipated that schools / academies will remove these sections from their final AUP document. Schools should review and amend the contents of this AUP to ensure that it is consistent with their E-Safety Policy and other relevant school policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUP will be more concise.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and

communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school (*schools / academies should amend this section in the light of their policies which relate to the use of school systems and equipment out of school*)
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (*schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems*)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (*schools / academies should amend this section to take account of their policy on access to social networking and similar sites*)

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school / academy equipment. I will also follow any additional rules set by the school / academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools / academies should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal email addresses on the school / academy ICT systems. (schools / academies should amend this section in the light of their email policy – some schools / academies will choose to allow the use of staff personal email addresses on the premises).
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies. (schools / academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy ICT equipment in school, but also applies to my use of school / academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools / academies should amend this section to provide relevant

sanctions as per their behaviour policies) a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name

Signed

Date

Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use Agreement

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

- I understand that my use of school / academy) systems and devices and digital communications will be monitored

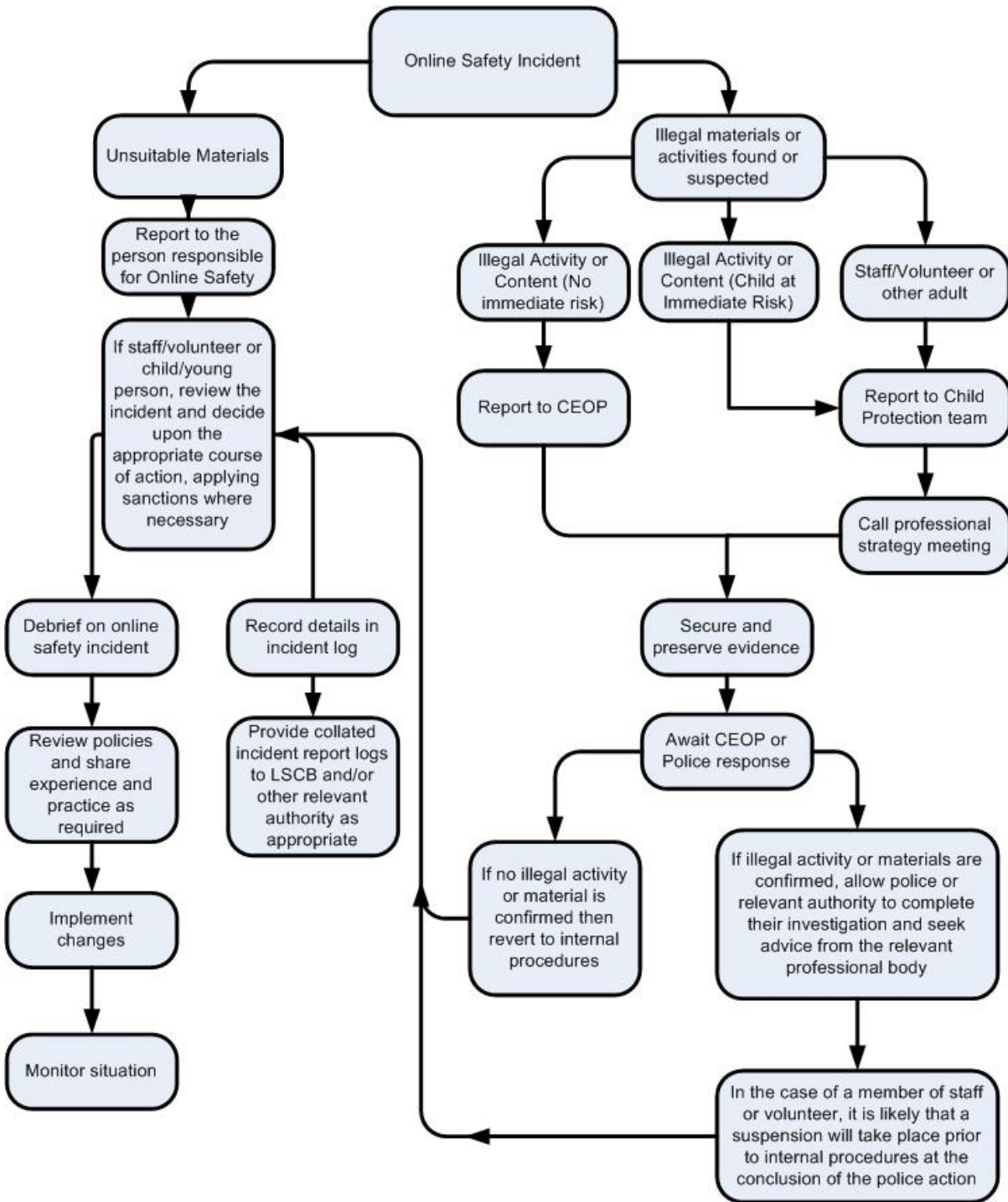
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school / academy has the right to remove my access to school systems / devices

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

Name

Signed Date

Responding to incidents of misuse – flow chart



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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

--

Web site(s) address / device Reason for concern

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Template Reporting Log

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

Training Needs Audit

Training Needs Audit Log Group	Date										
	Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date				

School Technical Security Policy Template (including filtering and passwords) - amended November 2013

Suggestions for use

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

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

Where sections are highlighted in BOLD text, it is the view of the SWGfL E-Safety Group that these would be an essential part of a school e-safety policy.

The template uses various terms such as school / academy; students / pupils. Users will need to choose which term to use for their circumstances and delete the other accordingly.

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.

If the *school / academy* 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 / academy* itself (as suggested below). It is also important that the managed service provider is fully aware of the *school / academy* E-Safety Policy / Acceptable Use Agreements). The *school / academy* 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 (insert title) (schools will probably choose the Network Manager / Technical Staff / Head of Computing or other relevant responsible person)

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: (schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:)

- **School / Academy technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements** (these may be outlined in Local Authority / other relevant body technical / e-safety policy and guidance)

- **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** (schools may wish to provide more detail) **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** (schools may wish to provide more detail).
- **All users will have clearly defined access rights to school / academy 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 E-Safety Committee (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. *(See Password section below).*
- *(Insert name or role)* 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 *(Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)*
- *Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems). (Schools / academies may wish to add details of the mobile device security procedures that are in use).*
- *School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (schools / academies may wish to add details of the monitoring programmes that are used).*
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place (to be described) for users to report any actual / potential technical incident to the E-Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).*
- *An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school system.*
- *An agreed policy is in place (to be described) regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)*
- *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. (see School Personal Data Policy Template in the appendix for further detail)*

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). Where sensitive data is in use – particularly when accessed on laptops – schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

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 E-Safety Committee (or other group).
- **All school / academy networks and systems will be protected by secure passwords that are regularly changed**
- **The “master / administrator” passwords for the school / academy systems, used by the technical staff must also be available to the Headteacher / Principal 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.**
- *(A school / academy should never allow one user to have sole administrator access)*
- *Passwords for new users, and replacement passwords for existing users will be allocated by xxxxx (insert title) (schools may wish to have someone other than the school’s technical staff carrying out this role eg an administrator who is easily accessible to users). Any changes carried out must be notified to the manager of the password security policy (above).*
- 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 in the staff and student / pupil sections below*
- *The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account)*
- *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 pupil / student)*

Staff passwords:

- **All staff users will be provided with a username and password** by *(insert name or title) 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 60 to 90 days (Some organisations require changes each month / 6 weeks. The frequency should depend on the nature of the account and how sensitive / damaging loss of data would be. It would be reasonable to require staff password changes more frequently than student / pupil password changes)*
- *should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used asswords created by the same user.*
- *should be different for different accounts, to ensure that other systems are not put at risk if one is compromised*
- *should be different for systems used inside and outside of school*

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 / academies* 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 / Academies 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 users (at KS2 and above) will be provided with a username and password** by *(insert name or title)* who will keep an up to date record of users and their usernames.
- *Users will be required to change their password every (insert period).*
- 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.

Schools / academies may wish to add to this list for all or some students / pupils any of the relevant policy statements from the staff section above.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

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

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

- in lessons *(the school should describe how this will take place)*
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (insert title) 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.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools / academies. Where available, schools / academies should 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.

Schools / academies need to consider carefully the issues raised and decide:

- Whether they 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.
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- **be logged in change control logs**
- **be reported to a second responsible person (insert title):**
- *either... be reported to and authorised by a second responsible person prior to changes being made (recommended)*
- *or... be reported to a second responsible person (insert title) every X weeks / months in the form of an audit of the change control logs*
- *be reported to the E-Safety Group every X weeks / months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) 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 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.

- *Either - The school / academy maintains and supports the managed filtering service provided by the Internet Service Provider (or other filtering service provider)*
- *Or – The school / academy manages its own filtering service (nb. If a school / academy decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the Headteacher / Principal would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff / students / pupils)*

- *The school has provided enhanced / differentiated user-level filtering through the use of the (insert name) filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / 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 / Principal (or other nominated senior leader).*
- *Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (insert name or title) (nb an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.*

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the e-safety education programme (schools may wish to add details). 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: (amend as relevant)

- *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. (amend as relevant)

Changes to the Filtering System

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

- *how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)*
- *the grounds on which they may be allowed or denied (schools may choose to allow access to some sites eg social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).*
- *how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)*
- *any audit / reporting 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 (insert title) who will decide whether to make school level changes (as above).

Monitoring

Some schools / academies supplement their filtering systems with additional monitoring systems. If this is the case, schools / academies should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

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: (details should be inserted if the school / academy so wishes).*

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- *the second responsible person (insert title)*
- *E-Safety Group*
- *E-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. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

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 Personal Data Handling Policy Template (amended November 2013)

Suggestions for use

Sections within this template are for information or guidance purposes only are shown in **BLUE**. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

The template uses the terms students / pupils to refer to the children or young people at the institution. Schools will need to choose which term to use and delete the other accordingly.

School Personal Data Handling Policy

Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your

systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

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

It is a statutory requirement for all schools to have a Data Protection Policy:

(<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools>)

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 (‘the DPA’). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

It is important to stress that the Personal Data Handling Policy Template applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall e-safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review this policy template and amend sections, as necessary, in the light of pertinent Local Authority regulations and guidance, and changes in legislation.

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

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”. (see [Privacy Notice section below](#))

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 *pupils / students*, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg 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 (insert name or title). (Schools may choose to combine this role with that of Data Protection Officer). 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) (the school may wish to identify these staff by name or title in this section) for the various types of data being held (eg pupil / 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 pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through ... (to be inserted – schools might choose to use the Prospectus, newsletters, reports or a specific letter / communication). Parents / carers of young people who are new to the school will be provided with the privacy notice through (to be inserted – as above).

More information about the suggested wording of privacy notices can be found on the DfE website:
<http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn>. A copy of the guidance is also included as an appendix the end of this template policy. LA Schools are advised to contact their Local Authority for local versions of the Privacy Notice and to check for annual updates.

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: (schools should amend or add to as necessary)

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners (or insert titles of relevant persons)

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 / pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, eg 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.

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

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

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information

when you have finished using it”.

Schools will need to review the above section with regard to LA policies (where relevant), which may be more specific, particularly in the case of HR records.

Secure Storage of and access to data

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

All users will use strong passwords which must be changed regularly (insert relevant school details as per the school's password security policy). 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 (where allowed)). Private equipment (ie 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 (many memory sticks / cards and other mobile devices cannot be password protected),
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- 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 will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.

The school / academy 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 will need to set its own policy, relevant to its physical layout, type of ICT systems etc)

The school / academy has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see appendix for further information and the ICO Guidance:

http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

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

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

The school / academy recognises that under Section 7 of the DPA, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> data subjects have a number of rights in connection with

their personal data, the main one being the right of access. Procedures are in place ([insert details here](#)) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

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

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

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance ([see earlier section for reference to the Cabinet Office guidance](#)), and other media must be shredded, incinerated or otherwise disintegrated for data.

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

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. ([insert name or title](#))

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: ([schools should determine their own reporting policy, in line with that of their LA \(if relevant\), and add details here](#))

- 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.

Use of technologies and Protective Marking

The following provides a useful guide:

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

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

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

New advice to schools will make clear that they will no longer be able to use pupils' biometric data without parental consent. The advice will come into effect from September 2013. Schools may wish to consider these changes when reviewing their Personal Data Handling Template. Schools may wish to incorporate the parental permission procedures into existing parental forms (eg AUP / Digital & Video Images permission form).

Use of Cloud Services

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

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

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

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

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

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

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

Parental permission for use of cloud hosted services

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

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

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

Privacy and Electronic Communications

Schools should be aware that the Privacy and Electronic Communications Regulations have changed and that they are subject to these changes in the operation of their websites.

Freedom of Information Act

All schools (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body.
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.
- Ensure that a well managed records management and information system exists in order to comply with requests.
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis.

Model Publication Scheme

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

Guidance on the model publication scheme can be found at:

http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx

The Schools Model Publication Scheme Template is available from:

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/schools_engl_and_mps_final.pdf

Guidance and a Model Publication Scheme for Academies can be found at:

<http://www.education.gov.uk/schools/leadership/typesofschools/academies/open/a00205178/freedom-of-information-guide-for-academies>

Further Guidance

ICO guidance can be found at the following link - including a pdf version - updated in September 2012:
http://www.ico.gov.uk/for_organisations/freedom_of_information/guide.aspx

DfE guidance that is specific to Academies can be found at:
<http://www.education.gov.uk/aboutdfe/foi/disclosuresaboutschoools/a0076171/academies-and-freedom-of-information>

<http://www.education.gov.uk/schools/leadership/typesofschoools/academies/open/a00205178/freedom-of-information-guide-for-academies>

Appendix - DfE Guidance on the wording of the Privacy Notice

PRIVACY NOTICE TEMPLATE
for
Pupils in Schools, Alternative Provision and Pupil Referral Units
and Children in Early Years Settings

(This is suggested text which can be amended to suit local needs and circumstances)

Privacy Notice - Data Protection Act 1998

We (**Name of school / academy / establishment**) are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

In addition for Secondary and Middle deemed Secondary Schools

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent's/s' name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please inform (*Insert name of School Administrator*) if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at www.direct.gov.uk/en/YoungPeople/index.htm or the LA website shown above.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

(For Academy use only) We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact **(Insert name of School Administrator)**.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

[Insert LA website link] and

<http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause>

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

[insert details and link to appropriate contact at the LA]

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT

Website: www.education.gov.uk

email: <http://www.education.gov.uk/help/contactus>

Telephone: 0370 000 2288

School Policy Template: Electronic Devices - Searching & Deletion (amended November 2013)

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

It is for each *school's / academy's Headteacher / Principal and Governors / Directors* to set, apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the school is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any school's policy on this or any other matter.

Within this template, sections which include information or guidance are shown in **BLUE**. It is anticipated that schools will remove these sections from their completed policy documents, though this will be for the school's relevant policy advisory group to recommend and for the head teacher and other governors to decide upon.

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

Where sections are highlighted in BOLD text, it is the view of the SWGfL E-Safety Group that these ought to be an essential part of a school e-safety policy.

The template uses the term students / pupils to refer to the children / young people attending the learning institution and the term Headteacher / Principal. Schools will need to choose which terms to use and delete the others accordingly.

Introduction

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

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

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

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

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

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

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

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

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>

It is recommended that Headteachers / Principals (and, at the least, other senior leaders) should be familiar with this guidance.

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 / Principal* 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/Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: [insert relevant names / roles / group](#)

The *Headteacher / Principal* 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: (the policy should here list those staff / roles given such authority. A Headteacher / Principal may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The *Headteacher / Principal* 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

It is essential that all staff should be made aware of and should implement the school's policy.

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 / Principal 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.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

Either:

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

Or

Pupils / students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. (you should refer to the relevant policy or to list here the conditions under which they are allowed)

If pupils / students breach these roles:

Either:

The sanctions for breaking these rules will be: (list here)

Or

The sanctions for breaking these rules can be found in the (name the policy - for many schools this will be 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 *student / pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties eg a visiting parent or contractor, only to devices in the possession of pupils / students.)

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 student / pupil being searched.

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

There is a limited exception to this rule: Authorised staff can carry out a search of a *student / 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 *student / pupil* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves). 'Possessions' means any goods over which the *student / pupil* has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments / headwear and may wish to refer to it in this policy)

A *student's / pupil's* possessions can only be searched in the presence of the *student / 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.

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

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities / LSCBs may also have further guidance, specific to their area.

Deletion of Data

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

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).

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

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

Audit / Monitoring / Reporting / Review

The responsible person (insert title) 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. (a template log sheet can be found in the appendices to the School E-Safety Template Policies)

These records will be reviewed by ... (*E-Safety Officer / E-Safety Committee / E-Safety Governor*) at regular intervals (*state the frequency*).

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance (*DfE guidance will be reviewed in 2013*) and evidence gained from the records.

The school is required to publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion.

School Bring Your Own Devices (BYOD) Template Policy

To be added

School Policy Template - E-Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the [school/ academy] community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

2. MEMBERSHIP

2.1 The e-safety committee will seek to include representation from all stakeholders.

The composition of the group should include *(NB in small schools one member of staff may hold more than one of these posts):*

[add/delete where appropriate]

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- *Student / pupil representation – for advice and feedback. Student / pupil voice is essential in the make up of the e-safety committee, but students / pupils 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 [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-ordinator (or other relevant person) with the following [add/delete where relevant]:

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through[add/delete as relevant]:
- Staff meetings
- Student / pupil forums (for advice and feedback)

- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

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 [\[insert name of organisation\]](#) have been agreed

Signed by (SLT):

Date:

Date for review:

Acknowledgement

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

Legislation

Schools should be aware of the legislative framework under which this 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 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 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 students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see [template policy in these appendices and for DfE guidance](#) -

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

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

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

Copyright of the SWGfL School E-Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in November 2013. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.