Ambler

Primary School and Children's Centre

Policy

e-safety Policy

September 2015

Next review with Safety, Service and Communications Committee September 2016

This policy is subject to on-going change and will be updated as and when required.

Distribution List

Copy Number	Name	Position	Organisation
Master	Business Manager		
Copy	Staff drive		

Introduction 5
Implementing the policy 5
What are the risks to children and staff? 5
Who does this policy apply to? 6
Review and monitoring 6
Roles and Responsibilities 8
Handling complaints 15
Communication and awareness 16
Communication with the whole school community 16
Communication with pupils 16
Communication with staff and staff training 16
Communication with parents and parent education 16
Policy statements 18
E-safety in the curriculum 18
Expected conduct 18
Use of communications technologies 21
Social media 21
Use of devices (including mobile phones) 22
Digital and video images in the school 25
Digital and video images in the children's centre 26
School website 27
Protecting personal data 27
Handling incidents 29
Technical statements: infrastructure, filtering and monitoring 32
Annexes 34

Acceptable use agreement: staff (and volunteers) 35
Acceptable use agreement: pupils - KS1.....37
Acceptable use agreement: pupils – KS2.....38
Acceptable use agreement: parents / carers.....39
Photography registration form (children's centre).....40
Sanctions in the event of an incident.....41
Responding to incidents of misuse: record of reviewing devices / internet sites 44
Template for incident log 46
Electronic Devices: Searching and deletion 47
Technical Security Policy.....51

Introduction

The purpose of this policy is to:

- set out the behaviours expected of all members of the school community at Ambler with respect to the use of the Internet and ICT-based technologies, and what will happen if these behaviours are not followed.
- safeguard and protect the children and staff of Ambler.
- set out clear structures to deal with on-line abuse such as cyberbullying.

Being safe on-line means protecting staff and children from many of the same risks that they face in the rest of their lives - such as being safe from bullying and discrimination - and ensuring that they can develop in a secure and stable environment.

This policy has been agreed by the senior leadership team and approved by Governors, and shared with other stakeholders such as the Friends of Ambler.

Positive behaviour on-line

Whilst this policy deals with many of the risks and dangers associated with digital technologies, at Ambler we welcome the opportunities these technologies offer to broaden horizons, enhance learning and connect pupils and staff with the wider world. The e-safety policy should be understood in a context where positive and constructive on-line behaviour is the norm, and is widely encouraged.

Implementing the policy

What are the risks to children and staff?

The main areas of risk for our school community can be summarised as follows:

Content

- Direct or indirect (inadvertent) exposure to inappropriate content, including on-line pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse/eating disorders/self-harm/suicide.
- hate sites
- ensuring that on-line content is authentic and accurate (e.g. protecting from fraud)

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and on-line reputation
- health and well-being (amount of time spent on-line internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) - upper KS2.
- copyright: ensuring pupils have a good understanding of the need to avoid plagiarism, respect other people's work and uphold copyright.

Who does this policy apply to?

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

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Ambler 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 Ambler, but are linked to membership of Ambler. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour and anti-bullying Policies.

Ambler will deal with such incidents within this policy and associated positive 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.

Review and monitoring

The e-safety policy is referenced from within other school policies: Computing policy, Safeguarding policy, Anti-Bullying policy, Positive Behaviour policy, Personal, Social and Health Education policy. Progress in implementing the policy is reflected in the Self-Evaluation Framework.

- The school has an e-safety co-ordinator who will be responsible for document ownership, review and updates.
- The e-safety co-ordinator is also responsible for ensuring that an action plan is in place to ensure that the policy is a 'live' document, used and referred to by all members of the Ambler community. This action plan will be reviewed by the e-safety governor on an annual basis.

This e-safety policy was approved by the Governing Body	*June 2015*
The implementation of this e-safety policy (including progress with the action plan) will be monitored by:	E-safety co-ordinator, and leadership team, supported by e-safety link governor (*for names, see Roles and Responsibilities below)*
The Governing Body will receive a report on the implementation of the e-safety policy generated by the e-safety co-ordinator (which will include anonymous details of e-safety incidents) at regular intervals. The following tools can be used for monitoring: • Incident log (see annex) • Logs of internet activity (including sites visited) • Surveys or questionnaires of staff, pupils and parents / carers	Once a term should incidents occur or at least once a year
The e-safety policy (and the action plan) 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. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff. The next anticipated review date will be:	May 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Headteacher, e-safety co-ordinator, designated safeguarding officer (Maria Glaster or other member of senior leadership team)

Roles and Responsibilities

Role	Responsibilities
Headteacher	• Overall responsibility for e-safety provision • Overall responsibility for data and data security • Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. London Grid for Learning (LGfL) • Responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • Is aware of procedures to be followed in the event of a serious e-safety incident. • Liaises regularly with the E-Safety Co-ordinator / Officer and have oversight of safety incident log • Ensures that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager) • Maintains an awareness of current e-safety issues and guidance through continuing professional development
E-safety Co-ordinator (Lucy Godfrey, yr 3 teacher – *until July 2015*)	• Oversees the delivery of the e-safety element of the computing curriculum • Ensures that e-safety education is embedded across the curriculum • Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing Ambler's e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • liaises with school ICT (Information and Communication Technology) technical staff • communicates regularly with SLT and the designated e-safety governor / committee to discuss current issues, review incident logs and filtering / change control logs • ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident

	• ensures that an e-safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies – where appropriate to curriculum rather than child protection issues (which will be referred to the designated child protection member of staff) • Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection 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 and use of social media

Governors / E-safety governor (Mary Stevens)	• A member of the Governing Body has taken on responsibility for overseeing e-safety. This governor will complete appropriate and ensure that s/he keeps up-to-date with any developments in this area. • S/he will work closely with the link governor for safeguarding. • Ensures that the school follows all current e-safety advice to keep the children and staff safe • Approves the e-safety policy and reviews the effectiveness of the policy. This will be carried out by the designated governor working closely with the e-safety co-ordinator and reporting to the Safety, Services and Communications Committee information about e-safety incidents and monitoring reports. • Supports the school in encouraging parents and the wider community to become engaged in e-safety activities and awareness.
Network manager / System administrator Greg Rochford)	• Reports any e-safety related issues that arise to the e-safety coordinator. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up-to-date • Ensures the security of the school ICT system • Ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • Ensures that the school's policy on web filtering is applied and updated on a regular basis and informs LGfL informed of issues relating to the filtering applied by the Grid • Keeps up to date with the school's e-safety policy and technical information • Ensures that the use of all relevant school systems (e.g. web site access, email use) is monitored in order that any misuse / attempted misuse can be reported to the e-safety co-ordinator and the headteacher for investigation / action / sanction • Ensures appropriate back-up procedures exist so that critical information and systems can be recovered in the event of a critical incident or breach. • Keeps up-to-date documentation of the school's e-security and

	technical procedures • Is the LGfL nominated contact

Business Manager (Marina Kilcoyne)	• Ensures that appropriate access controls are in place to protect pupils' data on the office equipment • Maintains an awareness of current e-safety issues and guidance through continuing professional development • Responds to e-safety concerns regarding external groups and ensures the completion of user agreements. Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
Staff responsible for delivering the curriculum	• Actively embed e-safety issues in all aspects of the curriculum and other activities • Ensure pupils understand and follow the e-safety and acceptable use policies • Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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, guide pupils to sites checked as suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches • When using digital images, inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
All staff	• Have an up-to-date awareness of e-safety matters and of the current school / academy e-safety policy and practices • Have read, understood and signed the Staff Acceptable Use Policy / Agreement • Must report any suspected misuse or problem to the headteacher and / or e-safety coordinator for investigation / action / sanction • Only use digital media to communicate with pupils / parents / carers be on a professional level and only using official school systems • Are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and

	implement current school policies with regard to these devices • Model safe, responsible and professional behaviours in their own use of technology

Pupils	• Read, understand, sign and adhere to the appropriate Pupil Acceptable Use agreement • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • understand the importance of reporting abuse, misuse or access to inappropriate materials • know how to be safe following the 'SMART steps to e-safety' (see KS1 Acceptable Use Agreement) and to know what action to take if they or someone they know feels worried or vulnerable when using on-line technology • know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • know and understand school policy on the taking / use of images and on cyber-bullying. • understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school • take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • help the school in the creation/ review of e-safety policies
Inclusion manager – responsible for parent engagement (Maria Glaster)	• Educates parents and raises awareness of e-safety on all levels in conjunction with e- safety coordinator and in response to emerging and current issues
Parents / carers	• Support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement at admission and reinforced in the Home school agreement • Read understand and promote the school Pupil Acceptable Use Agreement with their children • Consult with the school if they have any concerns about their children's use of technology at home and at school
External groups / volunteers	• Any external individual / organisation who is working alongside school staff will be supported by staff to adhere to the e-safety user agreement • Any external individual / organisation not working alongside

	Ambler staff will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Handling complaints

Ambler will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Our e-safety coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with child protection procedures (set out in the Safeguarding policy).

More detail of managing incidents is provided in the incident management section of this policy.

Communication and awareness

Communication with the whole school community

- Policy to be posted on the school website
- Key pointers are on display in the staffroom / classrooms and key areas (ICT hub, TECH lounge, office etc.)
- Acceptable use agreements to be issued to whole school community, on entry to the school and checked / renewed annually.

Communication with pupils

- All pupils sign an acceptable use agreement (for KS1 with their parent / carer) at entry to the school.
- Acceptable use agreements are checked and discussed with pupils at the start of each year.
- Key points displayed in classrooms

Communication with staff and staff training

- The e-safety coordinator, working with the business manager and the network managers, ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- The senior leadership team makes regular training available to staff on e-safety issues and the school's e-safety education program. A basic induction will take place on the first INSET of the autumn term in relation to minimum requirements and other training on an on-going and responsive basis as required.
- All new staff [including those on university/college placement and work experience] are provided with information and guidance on the e-safety policy and the school's Acceptable Use Policies as part of the induction process.
- Ambler holds signed acceptable use agreements in personnel files

Communication with parents and parent education

The inclusion manager, in conjunction with the e-safety coordinator arrange (in-house or with technical support as appropriate), arranges a rolling programme of advice, guidance and training for parents, including:

- Introduction of the acceptable use agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions held at school covering;
    - Suggestions for safe Internet use at home (e.g. advice on filtering systems and educational and leisure activities that promote responsible use of the Internet);
    - Information about national support sites for parents.

Policy statements

E-safety in the curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is 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.

Ambler has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This is on the shared network and there are currently three focussed lessons per year group across the year. Staff should also reinforce e-safety messages across the curriculum. There will also be additional e-safety reminders and focus activities where necessary and including being aware of its impact in homework.

The curriculum is guided by the following key principles:

- Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes should be in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Expected conduct

At Ambler we aim to ensure all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and in the curriculum.

There are acceptable use agreements for: staff (including temporary staff and volunteers), pupils and parents. These agreements are provided in the Annex. All users are responsible for using the school ICT systems in accordance with the relevant acceptable use

agreement which they will be expected to sign before being given access to school systems. In addition, all users:

- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- know and understand school policies on the use of mobile phones, digital cameras and hand-held devices
- understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- understand the importance of safeguarding data and protecting personal information (including passwords)
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand school policies on the taking / use of images and on cyber-bullying
- are informed that all Internet use may be monitored.

In addition, parents and carers:

- know how to report abuse, misuse or access to inappropriate materials, and how to raise a concern about any matter relating to e-safety
- understand the consequences of their child's misuse of digital technologies, and will support Ambler in taking action to address their child's behaviour

More information on handling incidents is set out in the incident management section.

The following table sets out the activities the school believes are inappropriate in a school context. Users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

		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	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

or pass on, material, remarks, proposals or comments that contain or relate to:	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 (e.g. offensive comments relating to comments on social media)				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				
Age-appropriate on-line gaming (non-educational)		X				
On-line gambling				X		
On-line shopping / commerce		X				

File sharing		X			
Use of social media (see social media section)		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

Use of communications technologies

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

- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging facilities or social media accounts must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Social media

The use of social media can blur the boundaries between private and professional identities, and as such presents challenges for staff and governors. At the same time, Ambler recognises that social networks provide important opportunities for parents, staff and governors to engage with peers, share knowledge and celebrate Ambler's achievements. In using social networking platforms staff, volunteers and governors should at all times ensure that they do not engage in any on-line activity that may compromise their professional responsibilities or Ambler's reputation.

Staff training will include: acceptable use of social media; social media risks; checking of settings; data protection; procedure for reporting issues.

Staff:

- will not run social network spaces for pupil use on a personal basis or open up their own spaces to their pupils, but, where social networking can enhance the curriculum, will use age-appropriate and approved systems for such communications.
- will not make reference in social media to pupils or parents / carers.
- will not engage in on-line discussion on personal matters relating to members of the school community
- will not befriend pupils or parents / carers on social networking sites
- should make it clear that they are all times expressing a personal opinion when engaging with social media in a personal capacity, and should refrain from posting material where there is any risk of ambiguity
- monitor and maintain security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Parents / carers and volunteers:

- will not make reference in social media to pupils (other than those for whom they are legally responsible), and will consider the possible impact of any posts relating to the Ambler community on wellbeing, privacy and security of everyone in that community. This includes not identifying or 'tagging' any photos of pupils, including in private groups (e.g. the Friends of Ambler facebook group). (See the digital images / video section for more information).
- wherever possible, will aim to engage with other Ambler parents in closed or private groups when using social networking sites.

Governors:

- The preferred system for governors to communicate internally with each other and share documents relating to Ambler is GovernorHub.

Use of devices (including mobile phones)

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 the use of personal devices that need to be reviewed prior to implementing such a policy. Use of personal devices should not introduce vulnerabilities into existing secure environments. The table below summarises the contexts in which personal devices may or may not be used.

It is not the intention to prevent parents/carers from taking pictures, but to ensure that photographic practices are monitored to reduce the risks of inappropriate photography/filming.[1]

No one is permitted to photograph or record images in the following areas:

- Changing areas
- Toilet areas
- First aid room
- Private spaces

In the children's centre:

- Managers must ensure that all staff members are aware they must not have mobile phones with them when they are working with children.
- Mobile phones must be kept in staff lockers or in staff rooms at all times and used only when staff members are on their breaks.
- Parents and carers should be informed that the emergency contact is the telephone number for the centre.
- If photographs or videos of children are to taken in the setting, they must be taken using the setting's own equipment. Staff should never take photos or videos of children using their own mobile phones or cameras

[1] Guidance taken from ISCB Safeguarding and Child Protection Policy and Procedures and adapted for early years settings (p15 Islington EY Safeguarding and Child Protection Procedures and Guidance).

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

The policy in relation to the searching for electronic devices, and the deletion of content as required is set out in the annex.

Staff and pupils are all reminded through training and/or the e-safety curriculum that the use of digital devices such as mobile phones can also present a physical risk to safety, for example by making users vulnerable to theft when using devices in outside environments. Pupils and staff are reminded of the importance of being aware of their environment at all times when using mobile phones and other handheld devices, including in areas (such as the streets immediately around Ambler) where there can be fast-moving vehicles.

Digital and video images in the school

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

The rules for the children's centre are slightly different. See below for more details

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- 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. To respect everyone's privacy and in some cases protection, parents should consider very carefully whether to make these images available on social networking sites. Parents and carers may share images of pupils on social media, but only with the express permission of the parents or carers of all the children concerned. They should be encouraged to do this in closed or private groups, wherever possible. Children must not be 'tagged' or identified under any circumstances, and parents should refrain from commenting on images or videos in ways that may make children identifiable. Where images could become publicly available no other children or staff must be identifiable, even if in the background.
- The school will work with Friends of Ambler to ensure that images shared on the private Friends of Ambler website / Facebook group e.g. of school events do not inadvertently enable protected children to be identified. The same rules about 'tagging' children apply in a private group.
- 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.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' surnames will not be used anywhere on a website or blog, particularly in association with photographs. First names can be used with permission e.g. for a media opportunity.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (annual agreement).
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. Recordings are handled in line with the data protection policy. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Digital and video images in the children's centre

Because of the greater vulnerability of younger children, the rules in the children's centre are slightly different.

- Children can only be photographed if permission of parents/carers is given (through the use of the digital consent form, available from the office).
- Any parent/carer wishing to take photographs/video which include other children (e.g. on a trip) should declare and sign an agreement that it is for family use only (see annex)
- Those taking photographs, including staff/volunteers must identify themselves.
- Photographers will be required to have formal identification which must be worn at all times.
- Children's images will not be used for promotional or press releases unless parents/carers have explicitly consented
- Unsupervised access to children or one-to-one photo sessions are prohibited
- Any concerns regarding inappropriate or intrusive photography/filming reported to, or observed by, the organiser of an event must be followed up by them with the person in question. If concerns persist this person can be requested to leave
- It is the responsibility of the manager to ensure assistants, volunteers and students adhere to this policy

Documenting events at the children's centre

In addition to the above:

- The centre will ask parents if they do not wish their children to be in any photographs/videos.
- The centre will be aware of any particular circumstances where photographic images should not be taken of an individual child.
- If there are parents that do not wish their children to be included in photograph/video then arrangements can be made at the end of the performance for photos to be taken by parents that do not include these children.

The digital image consent form is available from the school office and on the website.

School website

- The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: Head and deputy headteachers, ICT technician, business manager and school admin staff (*this point may need review in May 2016)*.
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the school address, telephone number and we use the school and children's centre office email contact address. We do not publish personal email addresses of pupils or staff on the school website.
- Photographs published on the web do not have names attached, with the exception of images specifically used to identify members of the Ambler team e.g. photos of staff and governors;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images

Protecting personal data

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.

All personal data is handled in accordance with the schools' data protection policy. The basic principles are summarised below.

The school ensures 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 the data protection / information sharing policy).
- All redundant equipment that may have held personal data will have the storage media wiped. Alternatively, if the storage media has failed, it will be physically destroyed. For the disposal of equipment Ambler will only use authorised companies who will supply a written guarantee that this will happen.

Staff must ensure that they:

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

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

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

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

Handling incidents

At Ambler incidents are dealt with in line with the flowchart set out below. The policy is intended to support and guide staff to manage incidents that involve the use of on-line services. Incidents might involve illegal or inappropriate activities (see 'Expected conduct' above).

At Ambler:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions (see annex)
- all members of the Ambler community are encouraged to be vigilant in identifying and reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the Local Authority and London Grid for Learning, UK Safer Internet Centre helpline, Child Exploitation and On-line Protection Centre)
- monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school.
- staff and pupils are informed that that they must report any failure of the filtering systems directly to the e-safety coordinator, who will liaise with the system administrator. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary;
- the records of incidents are recorded in the incident log and reported to the school's senior leaders, governors and the Local Authority (via the Local Authority Designated Office, as appropriate and in line with Ambler's safeguarding policy).
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we immediately refer any material we suspect is illegal to the appropriate authorities (the Police and the Local Authority).
- We will contact the Police if one of our staff or pupils receives on-line communication that we consider is particularly disturbing or breaks the law

Incident management procedure

All members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of

the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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 **report immediately to the police**.

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

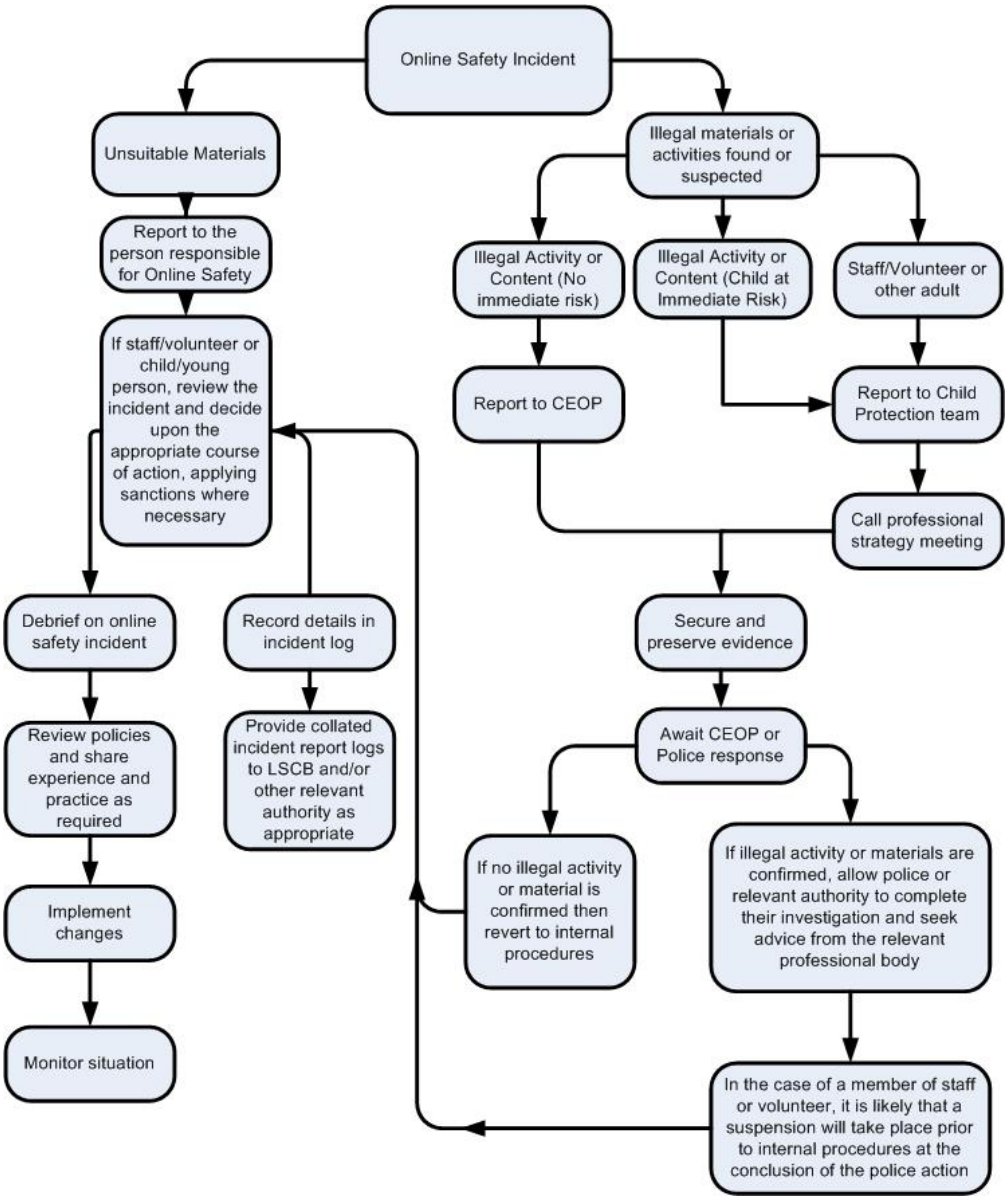
- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Use the form in the annex for recording the steps taken in an incident.
- Conduct the procedure using a designated computer that will not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

If content being reviewed **includes images of Child abuse then the monitoring should be halted and referred to the Police immediately**. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.



Technical statements: infrastructure, filtering and monitoring

Ambler 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.

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.

A more detailed Technical Security Policy can be found in the annex. Some general principles are provided below:

- There will be regular reviews and audits of the safety and security of school academy technical systems
- All users will be provided with a username and secure password by the ICT Co-ordinator who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has differentiated user-level filtering, to ensure that pupils only access age-appropriate content
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices, except in circumstances agreed with the systems administrator.

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see the section on protecting personal data)

Annexes

Acceptable use agreement: staff (and volunteers)

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 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 Ambler will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, virtual-learning environment etc.) out of school, and to the transfer of personal data (digital or paper-based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal use on an occasional basis, and will do so accordance with the policies and rules set down by the school in relation to expected conduct.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use social networking sites in school in accordance with the school's e-safety policy.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (tablets / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet bandwidth 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 I have permission)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the e-safety and data protection / information-sharing policies. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

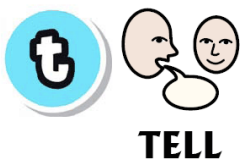
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Stay Safe be SMART

	I will keep safe by not giving out personal information online.
	I know online friends are strangers and will not meet up with anyone I have met online.
	I will only open messages and click on links when I know they are safe.
	I know not to believe everything I see and read online.
	If I see something I don't like on a screen, I will always tell an adult.
My Name:	

Acceptable use agreement: pupils – KS2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork (including clubs) and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Acceptable use agreement: parents / carers

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- ICT facilities and equipment at the school
- safe virtual learning environments and networks, as approved by the school

I also agree to support the school in encouraging the responsible use of ICT in the following ways:

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.	✓
I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.	✓
I will respect the privacy and safety of other children and staff by not making reference to them in social media without their express permission.	✓
I will consider the impact of any post on social media relating to Ambler on the wellbeing, privacy and security of everyone in the school community.	✓
If the school requests that I do not take photographs at an event then I will respect that decision.	✓
I will not share digital images of another child on social media without the express permission of the parents or carers of the child concerned. I will never 'tag' or identify other children or staff online. I will ensure that no other children could be identified unintentionally e.g. by appearing in the background.	✓
I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.	✓
I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns. I understand that the school will help to support me by providing appropriate information and training e.g. through coffee mornings.	✓

My daughter / son: _____

Parent / guardian signature: _____ **Date:** ___/___/___

Photography registration form (children's centre)

THIS FORM SHOULD BE COMPLETED BY ANYONE TAKING PHOTOGRAPHS

OR RECORDING IMAGES AT AN EVENT

I wish to take photographs or record images at this activity. I agree to abide by the organisers' guidelines and confirm that the photographs or recorded images will only be used for the purposes agreed with the activity organiser.

Name: _____

Address: _____

_____

_____

Tel No: _____

Signature: _____

Date: _____

Please return this registration form to the activity's organiser.

Sanctions in the event of an incident

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

Pupils **Actions / Sanctions**

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

Using proxy sites or other means to subvert the school's filtering system	X	X	X	?	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	?	X	?
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	?	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	?		X	X	?	X	?

Staff / volunteers **Actions / Sanctions**

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

pupils								
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's filtering system	X	X		?	X	X	?	?
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	?	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X			?	X		?
Continued infringements of the above, following previous warnings or sanctions	X	X				X	X	X

Responding to incidents of misuse: record of reviewing devices / internet sites

Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Template for incident log

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

Electronic Devices: Searching and deletion

Introduction

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

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

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

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

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

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

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

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents / carers and pupils at least once a year.

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for headteachers, staff and governing bodies"

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

Responsibilities

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

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

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

Training / Awareness

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

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

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

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

Policy Statements

Search:

This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are not allowed to bring mobile phones or other personal electronic devices to school. If pupils breach these roles:

Searching with consent - Authorised staff may search with the pupil's consent for any item.

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

In carrying out the search:

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

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

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

Extent of the search:

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

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

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

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

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.

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.

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.

Deletion of Data

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

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

A record should be kept of the reasons for the deletion of data / files (using the appropriate form).

Care of Confiscated Devices

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

Audit / Monitoring / Reporting / Review

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

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

Technical Security Policy

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 their findings have impact on policy and practice.

Technical Security

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

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

- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety coordinator
- 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).
- The business manager, working with 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
- Mobile device security and management procedures are in place
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate misuse system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy in the annex 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.

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 cloud services.

- 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 systems administrator and will be reviewed, at least annually.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the headteacher or other nominated senior leader and kept in a secure place e.g. school safe.
- Passwords for new users, and replacement passwords for existing users will be allocated by the systems administrator. Any changes carried out must be notified to the manager of the password security policy (above).
- All users (adults and children) 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 pupil sections below
- requests for password changes should be authenticated by systems administrator to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password by systems administrator who will keep an up-to-date record of users and their usernames.
- the password should contain a combination of letters and numbers.
- the password should 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 regularly (at least annually)
- 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

Pupil passwords

- Users will be required to change their password every year.
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children

Training / Awareness

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

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

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

- in lessons
- through the Acceptable Use Agreement

Filtering

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.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the school's ICT service provider. The provider will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

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

- be logged in change control logs
- be reported to a second responsible person (the e-safety coordinator)

All users have a responsibility to report immediately to the e-safety coordinator 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. The e-safety coordinator will liaise with the school's technical service provider and with the senior leadership team.

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.

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

Changes to the filtering system

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

Breaches of the filtering system will be dealt with in line the incident management procedure.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in this policy and the Acceptable Use Agreement. Monitoring will take place as follows:

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

- the second responsible person (e-safety coordinator)
- senior leadership team
- e-safety governor (s)
- external filtering provider / Local Authority / Police on request

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

Further Guidance

The following is recommended further guidance:

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