Online Safety Policies

This document includes the:

1. **School's Online Safety Policy, with agreed actions and sanctions for misuse**
2. **School's Technical Security Policy (including filtering and passwords)**
3. **School's Personal Data Handling Policy (Electronic)**
4. **School's Electronic Devices - Searching & Deletion Policy**

Review of these Online Safety Policies

The Online Safety Policies will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

The next anticipated review date will be: Spring Term 2018 (in light of changes to data protection)

These Online Safety policies have been developed by the St Bartholomew's Online Safety Group made up of:

- L. Jenner — Online Safety Subject Leader & PSHCE ed. Subject Leader
- C.Beckerson — Headteacher & Lead DSL
- W.England — Network Manager
- M.Simmons-Mears — Online Safety Link Governor
- M.Tims — Computing Subject Leader

The Online Safety Group provides a consultative group that has representation from the St Bartholomew's CofE (Aided) Primary School community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Acknowledgement

The St Bartholomew's Online Safety Group would like to acknowledge the SWGfL Online Safety Group whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy and of the 360 degree safe Online Safety Self Review Tool.

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

The **Education and Inspections Act 2006** empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The **2011 Education Act** increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour, anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Online Safety Policy Statements

Education – pupils

The education of pupils in Online Safety is an essential part of St Bartholomew's CofE (Aided) Primary School Online Safety provision. We understand that the children in our care need the help and support of the school to recognise and avoid Online Safety risks and build their resilience in an ever changing digital age.

Online Safety is a focus in all areas of the curriculum and staff reinforce Online Safety messages across the curriculum.

- an Online Safety curriculum has been planned and implemented as part of Computing/PSHCE ed. curriculums. The Online Safety curriculum from EYFS to Year Six is relevant, current and provides progression, being planned centrally by the Online Safety Subject Leader with opportunities for creative activities.
- key Online Safety messages are also reinforced through displayed posters and through our involvement in events such as Safer Internet Day/ Anti Bullying Week
- from Year Two pupils are taught to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- older pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- staff are required to act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Teachers will have pre-approved these sites in advance of the lesson.

Education – parents/carers

We understand that many parents and carers may have only a limited understanding of Online 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:

- letters, newsletters, our school website
- parents/carers sessions
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Visitors

We believe it is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- currently three members of the teaching staff have attended training and hold CEOP accreditation, L.Jenner, S.Avenell and C.Beckerson.
- a planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly by the Online Safety Group.
- all new staff receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- the Online Safety Leader and Computing Subject Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- this Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- the Online Safety Leader and Computing Subject Leader will provide advice / guidance / training to individuals as required.

Training – Governors

It is expected that governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology. This can be offered in a number of ways:

- attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL)/CEOP.
- participation in school training / information sessions for staff or parents

Bring Your Own Device (BYOD)

St Bartholomew's CofE (Aided) Primary School does not operate a separate BYOD Policy.

We appreciate that an expanding range of educational opportunities are offered by mobile technologies for teaching and learning. We have explored the impact of BYOD in introducing vulnerabilities into existing secure environments. At this time we therefore do not operate BYOD on the school premises.

We strongly recommend that no child makes their own way to and from school. In exceptional circumstances a Year Six child may be trusted by the family to do so. In such a case, for safeguarding, the school requires written parental instruction to be given in advance. We acknowledge that the family may require the child to carry a phone for the journey.

The school has therefore agreed in these instances that the following procedure is to be followed.

- Only Year Six pupils with written parental instruction in advance can carry phones if travelling alone;
- The pupil switches the mobile off at the bottom gate, when entering school grounds and must put the mobile in their bag immediately;
- At the classroom door they immediately hand the device to the teacher who must ensure the phone is switched off;
- The phone is sent to the front office with the register to be locked away for the duration of the school day, *(the school does not accept responsibility for the device).*
- At the end of the day the teacher sends for the phone, which is only handed back to the pupil at dismissal on the gate;
- All pupils must ensure that no phone is switched on whilst on school premises.

See agreed procedures for the use/misuse of technology for sanctions.

Social Media - Protecting our Professional Identity

All schools, have a duty of care to provide a safe learning environment for pupils and staff, we understand that schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, online bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

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

- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

School staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- any images/work documents should only be taken on school equipment, the personal equipment of staff should not be used for such purposes, to ensure images/identifiable references to pupils are not held on personal devices
- they must never add pupils as 'friends' in personal social media accounts (including past pupils up to the age of 16)
- are strongly advised not to add parents as friends to their personal social media accounts
- they should review and adjust their privacy settings to give them an appropriate level of privacy and confidentiality.

Use of Digital and Video Images

At St Bartholomew's we acknowledge that 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. 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.

However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. 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 to reduce the likelihood of the potential for harm:

- written permission from parents or carers for the publication of digital images will be obtained through the Parents/Carers Permission Form
- staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- when using digital images within the curriculum, 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
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Use of Digital / Video Images by Parents/Carers

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events **for their own personal use** (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on any social networking sites, nor should parents/carers comment on any activities involving other pupils/staff in the digital / video images.

The school will ensure parents are reminded of best practise through announcements and visible signage at school events.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Details are outlined in the school's Technical Security Policy (filtering and passwords).

Data Protection

Details are outlined in both the school's Data Protection Policy and the School's Personal Data Handling Policy (Electronic). Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states:

- 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.

Data Protection procedures will be reviewed in the Spring Term of 2018 to reflect on the changes in legislation with impending new General Data Protection Regulations (GDPR) set to be implemented in May 2018.

St Bartholomew's CofE (Aided) Primary School's

Technical Security Policy (filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. St Bartholomew's CofE (Aided) Primary School will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

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

Responsibilities

The management of technical security will be the responsibility of the School Network Manager.

The school will monitor the impact of this policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity

_____

Technical Security Policy Statements

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also 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 the Network Manager
- all users will have clearly defined access rights to school technical systems and devices.
- 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.

- our Network Manager/Headteacher are responsible for ensuring 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.
- 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 agreed reporting system (as outlined in the Agreed Procedures and Logs) is in place for users to report any technical incident/security breach. Records are to be kept centrally in the Online Safety log File.
- an agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.

Password Security

We understand that 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. The management of password security will be the responsibility of the School Network Manager.

Password Security Policy Statements

- all school networks and systems will be protected by secure passwords that are regularly changed
- the administrator passwords for the school systems used by the Network Manager is also available to a 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 Network Manager.
- users will change their passwords at regular intervals – as described in the staff and student / pupil sections below
- requests for password changes should be authenticated by the Network Manager to ensure that the new password can only be passed to the genuine user
- staff should use the 'lock' facility on laptops if they are leaving them unattended to protect data and documents

Staff passwords

- 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)
- are changed on a termly basis (this applies to both staff computer logons and staff email logons).
- staff are advised that passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- staff are advised that passwords should be different for systems used inside and outside of school
- volunteers/long term supply staff who require access to the school system will be provided with a logon with restricted access and therefore should not use the teacher's personal logon/password

Pupil passwords

- EYFS users are provided with a group user account by the Network Manager.
- all users (at Year One and above) are provided with a username and password by the Network Manager
- pupils will be taught the importance of password security

Training / Awareness

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

- at induction, through the school's Online Safety policy and through the Acceptable Use Agreement

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

- through computing lessons
- through the Pupils Acceptable Use Agreement

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 Online 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 Online Safety group. 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:

- be logged by the Network Manager
- and reviewed termly by the Online Safety Group

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 our filtering provider (BT Unicorn) 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.

- either - 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 BT Unicorn filtering programme.
- mobile devices that access the school internet connection (school) 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 Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware that their usage of the internet is filtered for their safety through the Online Safety lessons. Staff users will be made aware of the filtering systems through:

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

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions.

Audit / Reporting

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

St Bartholomew's CofE (Aided) Primary School's

Personal Data Handling Policy (Electronic)

This document should be read in conjunction with the school's Data Protection Policy which applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as this is part of an overall Online Safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

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.

Data Protection procedures will be reviewed in the Spring Term of 2018 to reflect on the changes in legislation with impending new General Data Protection Regulations (GDPR) set to be implemented in May 2018.

Introduction

We appreciate that our school and its 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.

We understand that 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.

Personal Data

St Bartholomew's CofE (Aided) Primary School follows the definitions of personal and sensitive data as outlined in the Data Protection Act (DPA). Personal Data held by the school relates to:

- personal information about members of the school community – including pupils / members of staff, parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- curricular / academic data e.g. class lists, pupil progress records, reports, references
- professional records e.g. employment history, taxation, 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.

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. 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.

- all personal data will be fairly obtained in accordance with the school's Data Protection Policy
- the school is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- the school has clear and understood arrangements for the security, storage and transfer of electronic personal data
- data subjects have rights of access and there are clear procedures for this to be obtained as outlined in the Data Protection Policy
- there are clear and understood routines for the deletion and disposal of data
- there is a known routine for reporting, logging, managing and recovering from information risk incidents

Staff must ensure that they:

- take care, at all times 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.
- only SLT members are permitted to synchronise personal mobile devices with the work email system
- this synchronisation is only permitted if the device complies with the school issued security policy, as defined by the Microsoft Office 365 mobile device management (MDM)

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 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

Information to Parents/Carers

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils of the data they collect process and hold on the pupils / the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed through a Fair Processing Notice.

Training & awareness

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

- induction training for new staff
- staff meetings / briefings / Inset

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:

- 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), 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 take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school;
- 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 i.e. residentials, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event, (as encrypted material is illegal in some countries).

St Bartholomew's CofE (Aided) Primary School's

Electronic Devices - Searching & Deletion Policy

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. 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 this policy is read in conjunction with the school's Agreed Procedures for the use or misuse of technology, which sets out clearly 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.

Responsibilities

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

In the event that a search of a pupil is required whilst on school premises, this policy stipulates that the Headteacher/SLT member is authorised to carry out searches for and of electronic devices, in the presence of another member of SLT staff. On school residentials/trips where the Headteacher/SLT may not be present the lead teacher of the trip is authorised to carry out searches for and of electronic devices.

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 Online Safety policy

Policy Statements

Year Six pupils with written permission from home are the only pupils permitted to bring a personal device onto the school premises; this should only happen with complete compliance to the rules laid down. Other than this St Bartholomew's does not operate a BYOD policy. If pupils breach these rules the sanctions can be found in the school's behaviour code.

- 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:

Authorised staff must refer to the guidelines as defined in the DfE Searching, Screening and Confiscation review Feb 2014 (updated July 2015)

Electronic Devices and Deletion of Data

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should inform parents, 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.

Authorised staff should refer to the agreed procedures and logs and guidance defined in the DfE Searching, Screening and Confiscation review Feb 2014 (updated July 2015)

Care of Confiscated Devices

School staff 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 Online Safety Governor and Headteacher annually and in response to changes in guidance and evidence gained from the records.