Hazel Slade Primary

Acting Principal: Mrs Sarah Camacho

HAZEL SLADE PRIMARY SCHOOL E-SAFETY POLICY

~~(Review date: Feb 2015)~~
~~Feb 2016~~
~~Feb 2017~~
~~Feb 2018 L..Stubbs~~
~~Feb 2019 L..Stubbs~~
~~July 2020 L..Stubbs~~
Oct 2020 H Jukes

Contents

Hazel Slade Primary Academy

E-Safety Policy

Hazel Slade Primary Academy E-Safety School Policy

Development / Monitoring / Review of this Policy

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

- *Acting Principal – Sarah Camacho*
- *E-Safety Officer / Coordinator – Sarah Camacho / Louise Stubbs and Hannah Jukes*
- *All Staff – including Teachers, Support Staff, Technical staff*
- *All Governors -*
- *Parents and Carers -*
- *Community users -*

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body:*	*TBA*
The implementation of this e-safety policy will be monitored by the:	*E- safety working group*
Monitoring will take place at regular intervals:	*Once per term*
Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Once per term*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Spring 2*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*E-safety Officer (SC/LS), DCPO (SC/LS/SS,DB) LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:
(SECURUS)

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

Hazel Slade Primary Academy E-Safety School Policy

Scope of the Policy

This policy applies to all members of the *school* (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 / academy*.

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

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

Roles and Responsibilities

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

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* ensure E-Safety is looked at along with Safeguarding of pupils. The role of the E-Safety *Governor.*

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors / Board / committee / meeting*

Headteacher and Senior Leaders:

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

Hazel Slade Primary Academy E-Safety School Policy

E-Safety Coordinator:

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

Network Manager / Technical staff:

The *Network Manager- Managed ICT provider*

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

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher / Senior Leader ; E-Safety Coordinator / Officer* for investigation / action / sanction**
- **all digital communications with pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Staying safe learning online.

1. Remote learning will only take place using **Microsoft Teams**.
    - **Microsoft Teams** has been assessed and approved by **the Principal - Sarah Camacho and the ICT Technician Steve Robinshaw**
2. Staff will only use **school** managed **or** specific, approved professional accounts with learners **and/or** parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted by staff members.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with **Sarah Camacho,** Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible **e.g. a school/setting laptop, tablet or other mobile device. If this is not provided, leaders should ensure clear expectations are in place in relation to safeguarding and data security when using personal devices e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.**
3. Online contact with learners **and/or** parents/carers will not take place outside of the operating times as defined by SLT:
    - **These times are between 9am and 4pm**
4. All remote lessons will be formally agreed; **a member of SLT, will be invited to all meetings and** is able to drop in at any time.
5. Live lessons taught through the remote sessions will only be held with approval and agreement from **the Acting Principal using Microsoft Teams**

Data Protection and Security

6. Any personal data used by staff and captured by **Microsoft Teams** when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy (**link**).
    - **No personal data will be used/stored.**
7. All remote learning and any other online communication will take place in line with current **Hazel Slade** confidentiality expectations as outlined in Data Protection, Confidentiality policy, Safeguarding Policy and ICT policy.
    - **Only Microsoft Office can be used to online teach pupils**
    - **Class List and Microsoft Office can be used to make contact with parents and pupils via messages**
    - **Two school adults must be present in all live teaching sessions**
    - **Clear neutral backgrounds must be behind staff when they are using Microsoft Teams**
8. All participants will be made aware that **Microsoft Teams** can record sessions. **Please note, consent from those involved in the session is required if settings are recording activity. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing data protection policy.**
9. Staff will not record lessons or meetings using personal equipment.
10. Only members of Hazel Slade community will be given access to **Microsoft Teams**.
11. Access to **Microsoft Teams** will be managed in line with current IT security expectations as outlined in **our ESafety Policy**

Session Management (Not all statements will be needed if settings are not delivering live content)

12. Staff will record the length, time, date and attendance of any sessions held.

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - **Detail specifics according to the system being used e.g. language filters, disabling/limiting chat, staff not permitting learners to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.**
14. When live streaming with learners:
    - contact will be made via learners' provided email accounts **through Microsoft Teams.**
    - contact will be made via a parents/carer account.
    - staff will mute/disable learners' videos and microphones.
    - At least 2 members of staff will be present.
        - If this is not possible, SLT approval will be sought.
15. Live 1 to 1 sessions will only take place with approval from the **Acting Principal and if there are no other options available**
16. A pre-agreed **invite** detailing the session expectations will be sent to those invited to attend and it will appear in that persons calendar
    - Access links should not be made public or shared by participants.
        - Learners **and/or** parents/carers should not forward or share access links.
        - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
17. Alternative approaches **or** access will be provided to those who do not have access.

Behaviour Expectations

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
19. All participants are expected to behave in line with existing **Hazel Slade Behaviour** policies and expectations. This also includes:
    - **Appropriate language will be used by all attendees.**
    - **Staff will not take or record images for their own personal use.**
    - **Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.**
20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
21. When sharing videos and/or live streaming, participants are required to:
    - **wear appropriate dress.**
    - **ensure backgrounds of videos are neutral (blurred if possible).**
    - **ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.**
22. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

23. Participants are encouraged to report concerns during remote **or** live streamed sessions:
    - **By using CPOMS – a new tab has been created called Remote Learning**
24. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to **the Acting Principal or Acting Vice Principal**
25. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
    - Sanctions for deliberate will include measures in place in the behaviour policy along with **restricting/removing use, contacting police if a criminal offence has been committed.**

Any safeguarding concerns will be reported to **Sarah Camacho**, Designated Safeguarding Lead, in line with our child protection policy.

Hazel Slade Primary Academy E-Safety School Policy

Digital Self Care

1. Encourage children and their adults to check the privacy settings on their computer to make sure they are safe and secure.
2. Review location services. Make sure you haven't accepted location on any apps you do not want it too be on.
3. Use wellbeing controls. Control the amount of time being used on computers particularly with online learning taking up most of the time.
4. Have an adult nearby children using the technology and not in a room where they cannot be seen by an adult.

Child Protection / Safeguarding Designated Person

All staff should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

E-Safety Group: E-safety CO (CPO), HT (CPO), ICT/E-safety Governor, LSA,

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

Members of the *E-safety Group* will assist the *E-Safety Coordinator*

- the production / review / monitoring of the school e-safety policy / documents.
- *the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.*
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

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

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

Policy Statements

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

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

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

- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications* see appendix for further links / resources)

Education – The Wider Community

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

- *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
- *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide e-safety information for the wider community*
- *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)*

Education & Training – Staff / Volunteers

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

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- *The E-Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

Hazel Slade Primary Academy E-Safety School Policy

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

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

Technical – infrastructure / equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users** (at KS2 and above) **will be provided with a username and secure password, Hazel Slade Academy** *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 term..*
- ***The " administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)***
- St Bart's Academy Trust along with Hazel Slade Academy are **responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **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 (see appendix for more details)
- *The school has provided enhanced / differentiated user-level filtering*
- *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, as agreed).*
- 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" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.*

- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

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

Use of digital and video images

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

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

use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.

- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website*
- *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection and GDPR

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

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

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - as GDPR regulators
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

Pupil data must not be removed from the school site and two bits of information can not be taken i.e. pupil names and date of birth

- **Transfer data using encryption and secure password protected devices.**

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

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

Communications

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

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	wed with staff permission	Not allowed
Mobile phones may be brought to school	√			x				
Use of mobile phones in lessons		√		x				
Use of mobile phones in social time		√		x				
Taking photos on mobile phones / cameras		√		x				
Use of other mobile devices eg tablets, gaming devices	√				√			
Use of personal email addresses in school, or on school network			√	x				
Use of school email for personal emails			√	x				
Use of messaging apps			√	x				
Use of social media		√		x				
Use of blogs	√				√			

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

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/ and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

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

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

User Actions	Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal

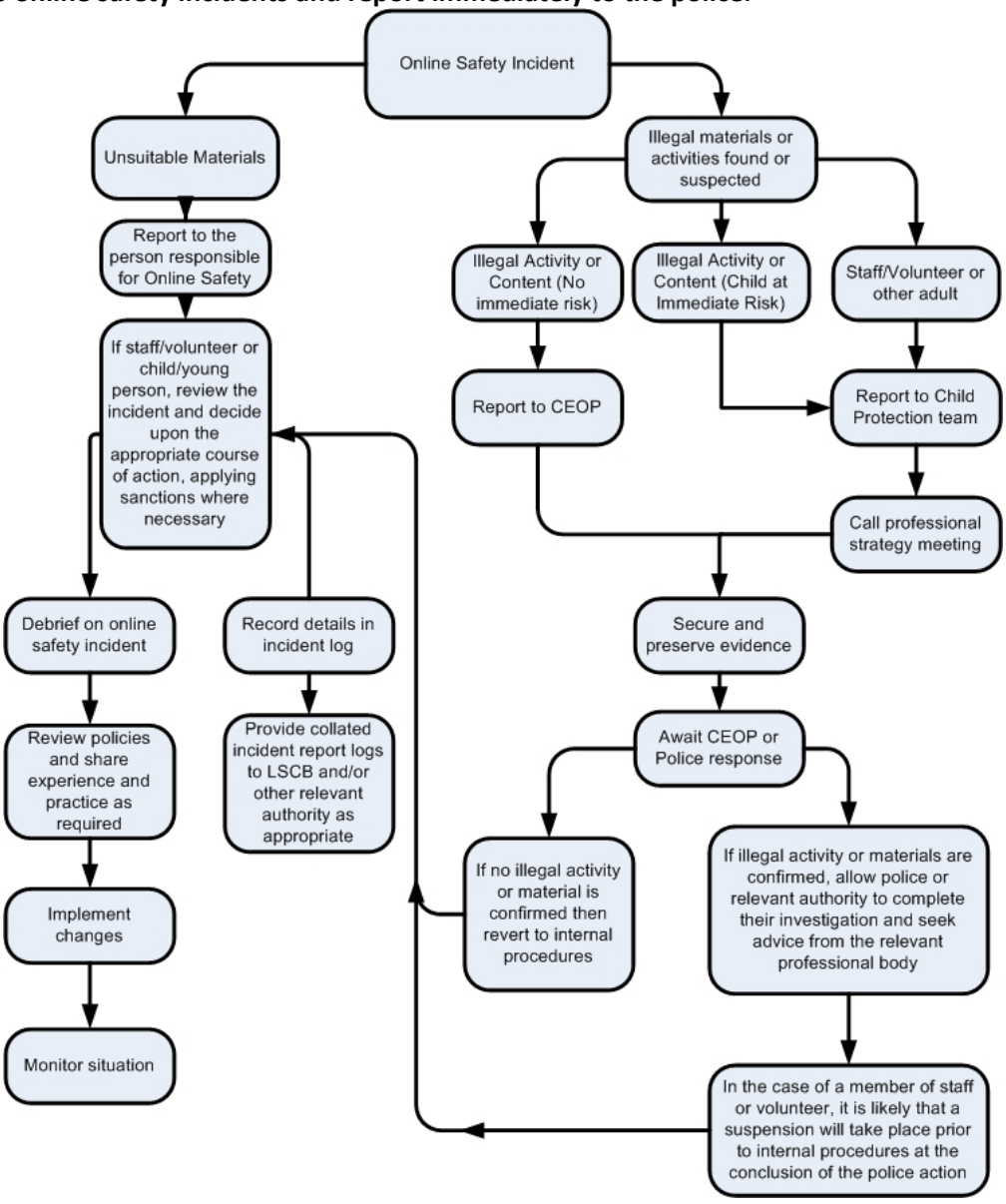
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection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

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that

members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions

Pupils

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

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√	√	√					
Using proxy sites or other means to subvert the school's filtering system		√	√	√					
Accidentally accessing offensive or pornographic material and failing to report the incident			√	√					
Deliberately accessing or trying to access offensive or pornographic material				√					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act				√	√				

Actions / Sanctions

Staff

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		√	√					
Unauthorised downloading or uploading of files		√	√					
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		√						
Careless use of personal data eg holding or transferring data in an insecure manner		√						
Deliberate actions to breach data protection or network security rules		√						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		√	√					
Using personal email / social networking / instant messaging / text messaging to		√	√					

carrying out digital communications with pupils								
Actions which could compromise the staff member's professional standing		√	√					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√	√					
Using proxy sites or other means to subvert the school's filtering system		√	√					
Accidentally accessing offensive or pornographic material and failing to report the incident		√	√					
Deliberately accessing or trying to access offensive or pornographic material		√	√	√				
Breaching copyright or licensing regulations		√	√					
Continued infringements of the above, following previous warnings or sanctions		√	√					

Appendix

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

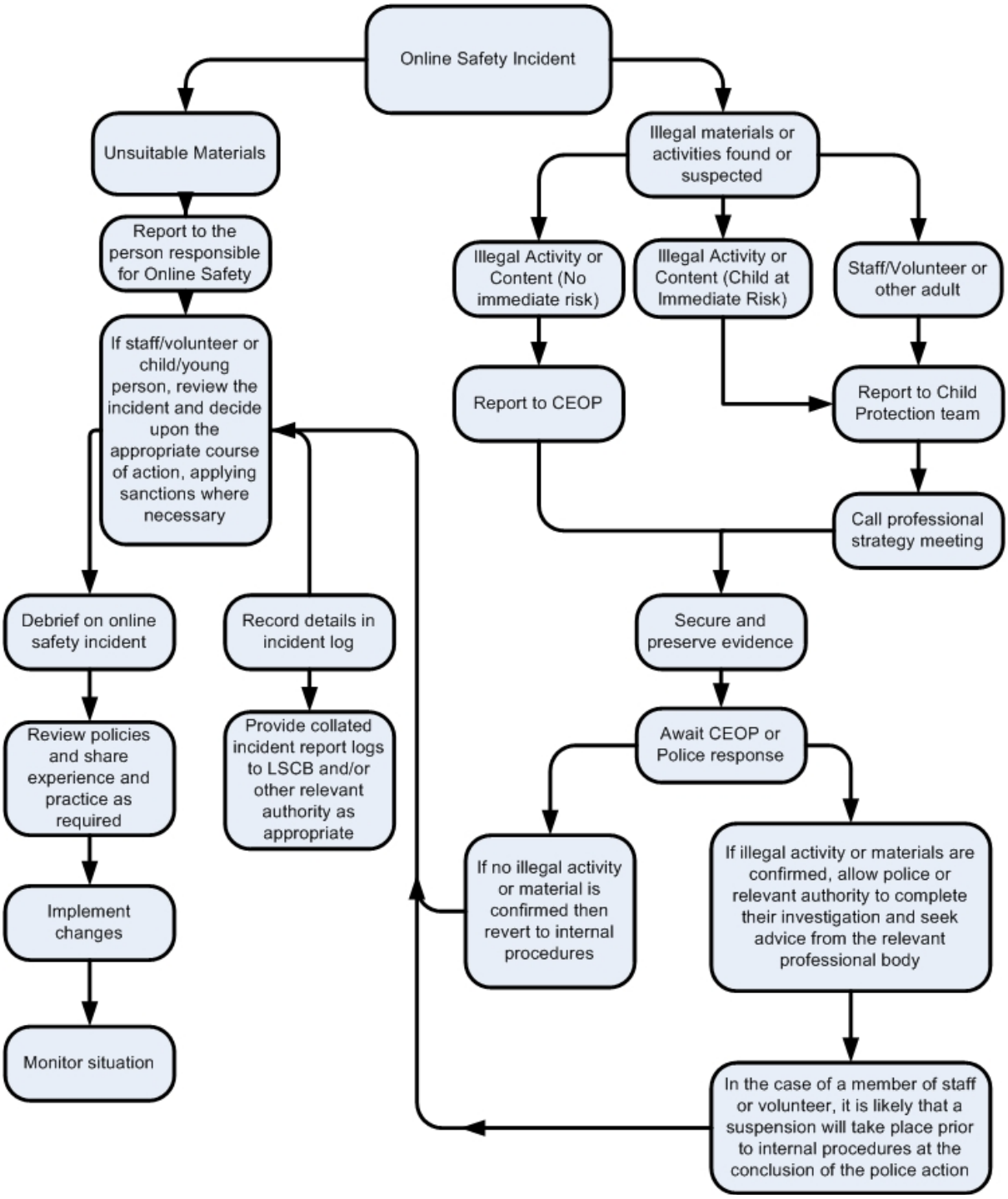
http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Acknowledgements

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

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

Responding to incidents of misuse – flow chart



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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

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

Conclusion and Action proposed or taken

Reporting Log

Reporting Log
Group .....

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

Training Needs Audit

Training Needs Audit Log

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

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

Hazel Slade Primary Academy E-Safety School 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 these have impact on policy and practice.

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

Responsibilities
The management of technical security will be the responsibility of the Academy ICT staff an the SLT at Hazel Slade.

Technical Security

Policy statements

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.**
- **There will be regular reviews and audits of the safety and security of school academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff/**.
- **All users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Academy IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- *Mobile device security and management procedures are in place (Mobile phone policy = Early Years)*
- *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 system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator / Technician (or other relevant person, as agreed).*
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy in the appendix for further detail)
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy in the appendix for further detail)

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- **All school 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 eg school safe. Consideration should also be given to using two factor authentication for such accounts**.
- A *school* should never allow one user to have sole administrator access
- *Passwords for new users, and replacement passwords for existing users will be allocated by the Academy IT Technician Technician. Any changes carried out must be notified to the manager of the password security policy (above).*
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Users will change their passwords at regular intervals – as described in the staff and pupil sections below*
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account)
- *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

Staff passwords:

- **All staff users will be provided with a username and password** by Academy IT Technician *who will keep an up to date record of users and their usernames.*
- *the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters*

- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous p *the last four passwords cannot be re-used* passwords created by the same user.
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Pupil passwords

- **All users** (at KS2 and above) **will be provided with a username and password** by *the Academy IT Technician who will keep an up to date record of users and their usernames.*
- *Users will be required to change their password every 90 days.*
- pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

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

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

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records are kept of:

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

Hazel Slade Primary Academy E-Safety School Policy

Filtering

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

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

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by ACADEMY IT TECHNICIAN. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

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 SS/CW:**
- *either... be reported to and authorised by a second responsible person prior to changes being made*
- *or... be reported to a second responsible person* SS/CW *every 4 weeks in the form of an audit of the change control logs*
- *be reported to the E-Safety Group every half term in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

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

- *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 filtering programme. Would like to add this…*

- *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. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.*

Education / Training / Awareness
Pupils will be made aware of the importance of filtering systems through the e-safety education programme . They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

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

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System
In this section the school should provide a detailed explanation of:

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

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

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows through regular* checks via SECURUS and technicians two weekly log.

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

- *the second responsible person* SS/CW
- *E-Safety Group*
- *E-Safety Governor*
- *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

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

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

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

School Personal Data Handling Policy

School Personal Data Handling Policy
Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

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

It is a statutory requirement for all schools to have a Data Protection Policy:
(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

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

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

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

Introduction
Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

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

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

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

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

Policy Statements
The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through : Prospectus, newsletters, reports or a specific letter / communication). Parents / carers of young people who are new to the school will be provided with the privacy notice as above.

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

Training & awareness

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

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

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

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	**Impact Level (IL)**	**Applies to schools?**
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

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

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

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

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

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to

them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

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

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media . Private equipment (ie owned by the users) must not be used for the storage of personal data.

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

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

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.

The *school* has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The *school* has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see appendix for further information and the ICO Guidance:
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

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

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

The *school* recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (insert details here) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

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

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA / school policies may forbid such transfer);

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

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

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

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

Audit Logging / Reporting / Incident Handling
It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. (ACADEMY IT TECHNICIAN)
The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking
The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

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

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

Use of Biometric Information

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

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

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

Use of Cloud Services

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

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

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

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

SWGfL provides a useful summary of these issues in a document that has been written with the support of Google and Microsoft:
http://www.swgfl.org.uk/News/Content/News-Articles/Cloud-based-products-and-services

Hazel Slade Primary Academy E-Safety School Policy

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

Parental permission for use of cloud hosted services

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

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

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

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

Freedom of Information Act

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

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

Model Publication Scheme

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

Guidance on the model publication scheme can be found at:
http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx

The Schools Model Publication Scheme Template is available from:
http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/schools_england_mps_final.pdf

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

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

Further Guidance

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

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

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

Appendix - DfE Guidance on the wording of the Privacy Notice

Hazel Slade Primary Academy E-Safety School Policy

School Policy: Electronic Devices 'Search and deletion'

Introduction

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

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

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

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

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

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

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

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

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

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

Relevant legislation:

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

- Human Rights Act 1998
- Computer Misuse Act 1990

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

Responsibilities

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

This policy has been written by and will be reviewed by E-safety committee.

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:
E-safety CO
AHT
E-safety committee member

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

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

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

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":
- at induction
- at regular updating sessions on the school's e-safety policy

Members of staff authorised by the Headteacher 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.