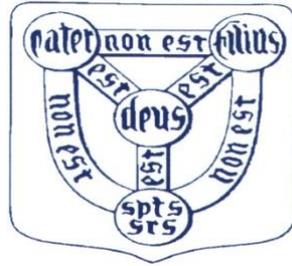# Shellingford CE (A) Primary School
## Headteacher: Miss Judith Terrell



"Inspiring hearts and minds"

# E-SAFETY POLICY

CONTENTS

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities
- Governors
- Headteacher / Senior Leaders
- E-Safety Co-ordinator
- Technical Staff / Contractors
- Teaching and Support Staff
- Child Protection / Safeguarding Designated Person
- Pupils
- Parents/Carers

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

**Appendices:**
- Pupil Acceptable Use Policy Agreement Template
- Parents/Carers Acceptable Use Policy Agreement Template

- Use of Digital / Video Images Agreement
- Staff Acceptable Use Agreement (incl. governors, external professionals and other regular volunteers)
- Occasional Visitors Acceptable Use Agreement
- Responding to incidents of misuse – flowchart
- School Reporting Log Template
- School Training Needs Audit template
- School Technical Security Policy template (includes password security and filtering)
- School Personal Data Policy template
- School Policy Template – Electronic Devices – Search and Deletion
- School Bring Your Own Devices (BYOD) Template Policy
- School E-Safety Group Terms of Reference
- Legislation
- Links to other organisations and documents
- Glossary of Terms

**Development / Monitoring / Review of this Policy**

This e-safety policy has been developed by a working group made up of:
- *Headteacher and E-Safety Co-ordinator*
- *Staff – including Teachers, Support Staff and Technical staff (Turn It On)*
- *Governing Body*
- *Parents/Carers*

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: | May 2021 |
| The implementation of this E-Safety policy will be monitored by the: | E-Safety Coordinator and Headteacher |
| Monitoring will take place at regular intervals: | At least once a year |
| The Governing Body will receive a report on the implementation of the E-Safety Policy: | As necessary |
| 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 of the policy will be: | May 2025 |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | Headteacher, E-Safety Coordinator |

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys or questionnaires of:    Pupils
      Parents/Carers
      Staff

## Scope of the Policy

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

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

The Headteacher 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. The designated governor for Child Protection and Safeguarding will also monitor e-safety which will include:

- *liaison with the E-Safety Co-ordinator*
- *monitoring of e-safety incident logs*
- *monitoring of filtering / change control logs*
- *reporting to relevant Governor meetings*

### 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 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 and Leadership team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher and Leadership team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and Leadership team will receive regular monitoring reports from the E-Safety Co-ordinator.

**E-Safety Coordinator will:**
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meet with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant Governor meetings
- report regularly to the Leadership Team

**Technical staff / Contractors:**
Shellingford CE (A) Primary School has a managed ICT service provided by an outside contractor 'Turn It On' and it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff. It is also important that the managed service provider is fully aware of the school e-safety policy and procedures.

The Technical Staff and ICT Co-ordinator is responsible for ensuring:
- **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 (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Leadership team; E-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- that recommendations are made to prevent any potential weaknesses in the technical infrastructure.

**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 for investigation / action / sanction**

- **all digital communications with pupil / 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 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

**Child Protection / Safeguarding Designated Person** should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying


**Pupils:**
- **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/Carers understand these issues through Parents/Carers' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents/Carers 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/Carers' sections of the website and on-line student records
- their children's personal devices in the school (where this is allowed)
- social media in relation to the school and staff

## 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 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, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (Turn It On) 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
Some parents/carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents/Carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to Parents/Carers through:
- Curriculum activities
- Letters, newsletters, website
- Parents/Carers evenings / sessions
- High profile events / campaigns e.g. 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 members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing information about 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/Carers.
- The school website will provide e-safety information for the wider community
- Supporting groups and organisations working in association with the school to enhance their e-safety provision

## Education & Training – Staff / Volunteers

Staff e-safety training supports understanding of 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.**
- **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 and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff at staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

## Training – Governors

**Governors should take part in e-safety training / awareness sessions,** with particular importance for those 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.
- Participation in school training / information sessions for staff or Parents/Carers

## Technical – infrastructure / equipment, filtering and monitoring

Shellingford CE (A) Primary School has a managed ICT service provided by an outside contractor (Turn It On); it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school E-Safety Policy and Acceptable Use Agreements. 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:

A more detailed Technical Security Template Policy can be found in the appendix.

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems and recommendations are made in order to comply with changing technologies**
- **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 will be provided with a username and secure password** by the ICT Subject Leader who will keep an up-to-date record of users and their usernames. **Users are responsible for the security of their username and password** and will be required to change their password every year
- **The "master / administrator" passwords for the school ICT system, used by the ICT Subject Leader must also be available to the Headteacher or other nominated leader and kept in a secure place**
- **The ICT Subject Leader 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**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has 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.
- Appropriate security measures are in place to protect the servers, firewalls, routers wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place 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 (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

**Bring Your Own Device (BYOD)**

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

management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive, and a BYOD Policy should be in place and reference made within all relevant policies. (see appendix for a more detailed BYOD Policy Template)

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the General Data Protection Regulations (GDPR) 2018 principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance and recommendations are made to keep up with changing technologies
- 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 e.g. on social networking sites**.
- In accordance with guidance from the Information Commissioner's Office, Parents/Carers are welcome to take videos and digital images of their own children at school events for their own personal use (as such use is not covered by the GDPR). To respect everyone's privacy and in some cases protection, these images should not be published or 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
    The school requires all parents to sign a Publicity Consent Form in respect of the following points:
    - Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
-

- Pupils' full names will not be used anywhere on a website or school blog, particularly in association with photographs.
- Written permission from Parents/Carers will be obtained before photographs or videos of pupils are published on the school website or a school blog

## General Data Protection Regulations (GDPR) 2018

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) 2018 which states that personal data must be:

- Processed lawfully, fairly and transparently
- Collected for explicit and legitimate purposes
- Adequate, relevant and limited
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in a secure manner

**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".** (see Privacy Notice section in the appendix)
- **It has a GDPR Data Protection Policy** (see separate policy)
- **It has a designated Data Protection Officer (DPO) in order to inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.**
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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

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

- the data must be encrypted and password protected
- the device must be password protected
- 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:

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

** 'Allowed at certain times' is defined as during break times from work; use of mobile devices, messaging apps, blogs and social media are not allowed during any educational activity involving pupils or duties including the supervision of pupils e.g. After-School clubs, playtime duties. During school hours all emergency calls should be directed through the school's landline or mobile telephone.

-

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and Pupils or Parents/Carers (email, 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.***
- *Pupil's at KS2 and above may 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

The school should ensure that:

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

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

| | | | | | |
|---|---|---|---|---|---|
| On-line gaming (educational) | | | | X | |
| On-line gaming (non educational) | | | | X | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | X | | | |
| File sharing | | X | | | |
| Use of social media | | X | | | |
| Use of messaging apps | | X | | | |
| Use of video broadcasting e.g. YouTube | | | | X | |

** 'Acceptable at certain times' is defined for staff during break times from work.

**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 website(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.**

**Online Safety Incident** flowchart:

- Online Safety Incident
  - **Unsuitable Materials**
    - Report to the person responsible for Online Safety
    - If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
      - Debrief on online safety incident
        - Review policies and share experience and practice as required
          - Implement changes
            - Monitor situation
      - Record details in incident log
        - Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
  - **Illegal materials or activities found or suspected**
    - Illegal Activity or Content (No immediate risk)
      - Report to CEOP
    - Illegal Activity or Content (Child at Immediate Risk)
      - Report to Child Protection team
    - Staff/Volunteer or other adult
      - Report to Child Protection team
        - Call professional strategy meeting
          - Secure and preserve evidence
            - Await CEOP or Police response
              - If no illegal activity or material is confirmed then revert to internal procedures
              - If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
                - In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

**Other Incidents**

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 / governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer (Headteacher's) 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:

## Pupils

| Incidents: | Refer to class teacher | Refer to Headteacher | Inform Governor Body | Seek Local Authority advice | 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 e.g. exclusion |
|---|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | X | X | X | X | X | | X |
| Unauthorised use of non-educational sites during lessons | X | X | | | | X | X | | X | |
| Unauthorised use of mobile phone / digital camera / other mobile device | X | X | | | | | X | | X | |
| Unauthorised use of social media / messaging | X | X | | | | | X | | X | |

| Incident | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| apps / personal email | | | | | | | | | |
| Unauthorised downloading or uploading of files | X | X | | | | X | X | | X | |
| Allowing others to access school network by sharing username and passwords | X | X | | | | X | X | | X | |
| Attempting to access or accessing the school network, using another pupil's account | X | | | | | | X | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | | X | | | | | X | | X | |
| Corrupting or destroying the data of other users | | X | X | X | | X | X | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | X | | | X | | X | X |
| Continued infringements of the above, following previous warnings or sanctions | | | X | X | X | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | X | X | | | | | | |
| Using proxy sites or other means to subvert the school's filtering system | | X | | | | X | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | X | | X | X | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR | | X | | X | | X | | | | |

** A 'Warning' may be followed by further sanctions, e.g. exclusion

**Staff**                                                        **Actions / Sanctions**

| Incidents: | Refer to Headteacher | Inform Governing Body | Seek Local Authority advice | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning ** | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | X | X | X | X | | X | | |
| Inappropriate personal use of the internet / social media / personal email | X | | X | | | X | | |
| Unauthorised downloading or uploading of files | X | | X | | | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | | | | | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | | | | X | X | | |
| Deliberate actions to breach data protection or network security rules | X | X | X | | | X | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | X | X | | X | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with Pupils | X | X | | | | X | | |
| Actions which could compromise the staff member's professional standing | X | X | X | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | | X | | | X | | |
| Using proxy sites or other means to subvert the school's filtering system | X | | | | | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | X | | | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | | | | X |
| Breaching copyright or licensing regulations | X | | X | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X | | | | | X |

** A 'Warning' will be followed by a suspension or disciplinary action if incident is repeated. Police may be involved.

*This policy was approved remotely by the Curriculum Committee on 19th May 2021 due to the current COVID-19 circumstances.*

**Date written: May 2021**              **Review Date: May 2024**

**Policy Agreed by the Governing Body on** ……………………….…………………….

**Signed** ………………………………………….. **Chair of Governing Body**

**Signed** …………………………………………. **Headteacher**

## Appendix

## Appendices

Can be found on the following pages:

•

# Pupil Acceptable Use Agreement

## Shellingford CE (A) Primary School

"Inspiring hearts and minds"

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

**THIS AGREEMENT TO BE DISCUSSED WITH PARENTS AND THEN SIGNED BY EACH INDIVIDUAL PUPIL.**

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

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

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

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

**I understand that everyone has equal rights to use technology as a resource and:**
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, social networking or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

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

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

-

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

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

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

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

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

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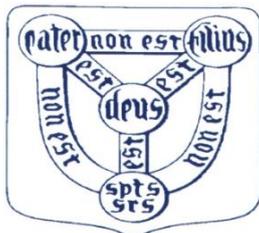
| Name of Pupil | |
|---|---|
| Group / Class | |
| Signed | |
| Date | |

# Parent/Carer Acceptable Use Agreement

## Shellingford CE (A) Primary School

"Inspiring hearts and minds"

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

**This Acceptable Use Policy is intended to ensure:**

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

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

Parents/Carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

**Permission Form**

| Parent / Carers Name | | Pupil Name | |
|---|---|---|---|

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

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

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

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
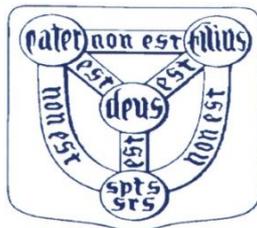
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed [                    ]    Date [            ]

Signed

# Use of Digital/Video Images Agreement

## Shellingford CE (A) Primary School

"Inspiring hearts and minds"

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

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

The school will comply with the General Data Protection Regulations (GDPR)and request Parents/Carers permission before taking images of members of the school.  We will also ensure that when images are published that the young people can not be identified by the use of their full names.

In accordance with guidance from the Information Commissioner's Office, Parents/Carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the GDPR). 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.

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

### Digital / Video Images Permission Form

| Parent / Carers Name | |
|---|---|
| Student / Pupil Name | |

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

Yes / No

I agree that if I take digital or video images at, or of, Shellingford CE (A) Primary School events which include images of children, other than my own, I will abide by these guidelines in my use of these images.
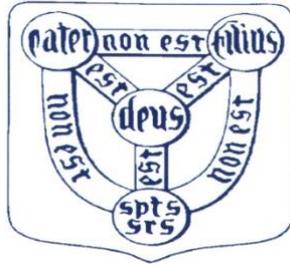
Yes / No

| Signed | | Date | |
|---|---|---|---|

# Staff Acceptable Use Agreement

**(including governors, external professionals and other regular volunteers)**

## Shellingford CE (A) Primary School



"Inspiring hearts and minds"

**School Policy**

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.  All users should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that staff, governors and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff are protected from potential risk in their use of ICT in their everyday work.

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

**Acceptable Use Policy Agreement**

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

**For my professional and personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

-

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

**I will be professional in my communications and actions when using school ICT systems:**
- I will not use my personal devices (tablet / laptop / mobile phone etc) for any school related work. *staff only
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with Pupils and Parents/Carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

•

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school policies.  Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that GDPR Data Protection Policy requires that any staff, governor or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

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

Staff / Governor / Volunteer Name

Signed

Date

# Occasional Visitors

# Acceptable Use Agreement

## Shellingford CE (A) Primary School
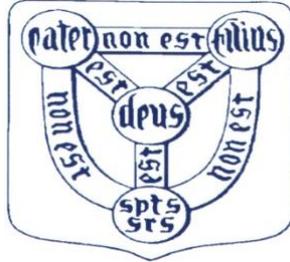


"Inspiring hearts and minds"

**This Acceptable Use Agreement is intended to ensure:**
- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

**Acceptable Use Agreement**
I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school
- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.

- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school / academy has the right to remove my access to school systems / devices

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

Name

Signed                                                    Date

## Responding to incidents of misuse – flow chart

```
                          Online Safety Incident
                         /                        \
          Unsuitable Materials          Illegal materials or
                  |                      activities found or
          Report to the                       suspected
      person responsible         /              |              \
        for Online Safety    Illegal Activity   Illegal Activity   Staff/Volunteer or
                  |           or Content (No     or Content (Child   other adult
       If staff/volunteer    immediate risk)    at Immediate Risk)       |
         or child/young            |                   |           Report to Child
       person, review the    Report to CEOP            |           Protection team
       incident and decide                             |                 |
             upon the                              Report to Child   Call professional
       appropriate course                         Protection team   strategy meeting
       of action, applying                                                |
         sanctions where                                           Secure and
           necessary                                             preserve evidence
          /        \                                                     |
   Debrief on    Record details                                  Await CEOP or
   online        in incident log                                 Police response
   safety                |                                        /         \
   incident      Provide collated                     If no illegal    If illegal activity
      |          incident report logs                 activity or      or materials are
   Review        to LSCB and/or                       material is      confirmed, allow
   policies      other relevant                       confirmed then   police or relevant
   and share     authority as                         revert to        authority to
   experience    appropriate                          internal         complete their
   and practice                                       procedures       investigation and
   as required                                                         seek advice from
      |                                                                the relevant
   Implement                                                           professional body
   changes                                                                  |
      |                                                            In the case of a
   Monitor                                                         member of staff
   situation                                                       or volunteer, it is
                                                                   likely that a
                                                                   suspension will
                                                                   take place prior
                                                                   to internal
                                                                   procedures at the
                                                                   conclusion of the
                                                                   police action
```

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

| Group | |
|---|---|
| Date | |
| Reason for investigation | |

### Details of first reviewing person

| Name | |
|---|---|
| Position | |
| Signature | |

### Details of second reviewing person

| Name | |
|---|---|
| Position | |
| Signature | |

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

| |
|---|

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

| | |
|---|---|
| | |
| | |
| | |
| | |

### Conclusion and Action proposed or taken

| | |
|---|---|
| | |
| | |
| | |
| | |

**Template Reporting Log**

Reporting Log
Group ...............

| Date | Time | Incident | Action taken | | 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 |
|------|----------|-------------------------------------|--------------------------|---------------|------|-------------|
|      |          |                                     |                          |               |      |             |
|      |          |                                     |                          |               |      |             |
|      |          |                                     |                          |               |      |             |
|      |          |                                     |                          |               |      |             |
|      |          |                                     |                          |               |      |             |
|      |          |                                     |                          |               |      |             |

## Training Needs Audit

# School Technical Security Policy Template (including filtering and passwords)

## Introduction

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

- users can only access data to which they have right of access
- shared and individual data folders are set correct permissions appropriately
- 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
- Monitoring logs are maintained and reported on where necessary
- 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.

## Responsibilities

The management of technical security will be the responsibility of the leadership team and Turn IT On

## 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 technical systems and recommendations are made to comply with changing technologies.**
- **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 Technical Staff / Contractor (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below).

- *Turn IT On is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations*
- *Mobile device security and management procedures are in place*
- *School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *Remote management tools are used by staff to control workstations and view users activity when appropriate.*
- *An appropriate misuse system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator (or other relevant person, as agreed).*
- *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 (e.g. 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 online malicious threats in the form of viruses, malware 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 and cloud services.

## 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 Technician and will be reviewed, at least annually.
- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe.**
- Passwords for new users, and replacement passwords for existing users will be allocated by Tom Watson (ICT 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 student / pupil sections below
- 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 student)

## Staff passwords:
- **All staff users will be provided with a username and password** by the *(Headteacher, School Administrator or Turn IT On Consultant) 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

## Student passwords
- **All users will be provided with a username and password** by the ICT Co-ordinator *who will keep an up-to-date record of users and their usernames.*
- *Users will be required to change their password every year.*
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

## Training / Awareness
Members of staff will be made aware of the school's password policy:
- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

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 (ICT Co-ordinator) will ensure that full records are kept of:
- User Ids and requests for password changes
-

- *User log-ons*
- *Security incidents related to this policy*

## Filtering

### Introduction

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

### Responsibilities

The responsibility for the management of the school's filtering policy will be held by Turn IT On. 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** (Turn It On Consultant)

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

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

### Policy Statements

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

- *Either - The school maintains and supports the managed filtering service provided by the Internet Service Provider*
- *Or – The school manages its own filtering service*
- *The school has provided enhanced / differentiated user-level filtering through the use of the* Sophos *filtering programme.*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (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 (*Turn It On*). *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Headteacher / Governors.*

## Education / Training / Awareness

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

## Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (*Turn It On*) 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:*

## Audit / Reporting

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

- *the second responsible person* (Turn It On)
- *E-Safety Governor / Governors committee*
- *External Filtering provider / Local Authority / Police on request*

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

## 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 / academy uses external providers for its technical support / security: http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx

# School Personal Data Policy Template

## 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).

## 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, members of staff and Parents/Carers / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by Parents/Carers / carers or by other agencies working with families or staff members.

## Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Headteacher. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- manage and address risks and will understand:
  - what information is held, for how long and for what purpose
  - how information has been amended or added to over time, and
  - who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

## Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

## Information to Parents/Carers / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the GDPR, the school will inform Parents/Carers / 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 (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to Parents/Carers / carers through newsletters, reports or a specific letter / communication. Parents/Carers / carers of young people who are new to the school will be provided with the privacy notice through newsletters, reports or a specific letter / communication.

## Training & awareness

All staff will receive data handling awareness / GDPR 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 Senior Information Risk Officer (SIRO)

## Risk Assessments

Information risk assessments will be carried out by the Senior Information Risk Officer (SIRO) 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

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 e.g. "Securely delete or shred this information when you have finished using it".

## 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 (i.e. owned by the users) must not be used for the storage of personal data.

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

- the data must be encrypted, and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking 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 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 General Data Protection Regulations (GDPR). The school will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

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 the GDPR 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 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
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- 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 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

## 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, 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.

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
• a plan of action of non-recurrence and further awareness raising.

All significant data protection breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours.

## School Policy Template: Electronic Devices - Searching & 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 Headteacher must publicise the school behaviour policy, in writing, to staff, Parents/Carers / 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

## Responsibilities

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

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

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

## Training / Awareness

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

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

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

## Policy Statements

## Search:

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

Pupils are allowed to bring mobile phones or other personal electronic devices to school in agreement with the Headteacher and use them only within the rules laid down by the school (e.g. handed in at reception and not taken anywhere else)

If pupils breach these roles:

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

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

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

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

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

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

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

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

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

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

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

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

### Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

**If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:**
- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

### Deletion of Data

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

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

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

### Care of Confiscated Devices

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

### Audit / Monitoring / Reporting / Review

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

These records will be reviewed by a Governor at least annually.

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

## Legislation

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

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

## Computer Misuse Act 1990

This Act makes it an offence to:
- Erase or amend data or programs without authority
- Obtain unauthorised access to a computer
- "Eavesdrop" on a computer
- Make unauthorised use of computer time or facilities
- Maliciously corrupt or erase data or programs
- Deny access to authorised users.

## General Data Protection Regulation (GDPR) 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
- Processed lawfully, fairly and transparently
- Collected for explicit and legitimate purposes
- Adequate, relevant and limited
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in a secure manner

## Freedom of Information Act 2000

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

## Communications Act 2003

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

## Malicious Communications Act 1988

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

## Regulation of Investigatory Powers Act 2000

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

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

## Trade Marks Act 1994

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

## Copyright, Designs and Patents Act 1988

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

## Telecommunications Act 1984

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

## Criminal Justice & Public Order Act 1994

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

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

## Racial and Religious Hatred Act 2006

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

## Protection from Harassment Act 1997

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

## Protection of Children Act 1978

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

## Sexual Offences Act 2003

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

## Public Order Act 1986

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

## Obscene Publications Act 1959 and 1964

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

## Human Rights Act 1998

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

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

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

## The Education and Inspections Act 2006

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

## The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

## The Protection of Freedoms Act 2012

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

## The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

## Links to other organisations or documents

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

## UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

## CEOP

http://ceop.police.uk/                    ThinkUKnow

## Others:

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

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

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

## Support for Schools

Specialist help and support   SWGfL BOOST

## Cyberbullying

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

Scottish Government  Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

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

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

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

## Social Networking

Digizen – Social Networking

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents/Carers Guide to Facebook](#)

[Facebook Guide for Educators](#)

## Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - [http://www.educationscotland.gov.uk/usingglowandict/](http://www.educationscotland.gov.uk/usingglowandict/)

Alberta, Canada - [digital citizenship policy development guide.pdf](#)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - [Education Resources](#)

Somerset - [e-Sense materials for schools](#)

## Mobile Devices / BYOD

Cloudlearn Report  [Effective practice for schools moving to end locking and blocking](#)

NEN   - [Guidance Note - BYOD](#)

## General Data Protection Regulations (GDPR)

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[ICO pages for young people](#)

[Guide to General Data Protection Regulations - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

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

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

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL -    Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

## Professional Standards / Staff Training

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

Kent -    Safer Practice with Technology

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

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

UK Safer Internet Centre Professionals Online Safety Helpline

## Infrastructure / Technical Support

Somerset -  Questions for Technical Support

NEN -  Guidance Note - esecurity

## Working with Parents/Carers and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

 SWGfL BOOST Presentations - Parents/Carers presentation

Connect Safely - a Parents/Carers Guide to Facebook

Vodafone Digital Parents/Carers Magazine

Childnet Webpages for Parents/Carers & Carers

[DirectGov - Internet Safety for Parents/Carers](#)

[Get Safe Online - resources for Parents/Carers](#)

[Teach Today - resources for Parents/Carers workshops / education](#)

[The Digital Universe of Your Children - animated videos for Parents/Carers (Insafe)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents/Carers' Guide](#)

[Insafe - A guide for Parents/Carers - education and the new media](#)

[The Cybersmile Foundation (cyberbullying) - advice for Parents/Carers](#)

## Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - it's not chalk and talk anymore!"](#)

## Glossary of terms

| | |
|---|---|
| AUP | Acceptable Use Policy – see templates earlier in this document |
| CEOP | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| CPC | Child Protection Committee |
| CPD | Continuous Professional Development |
| CYPS | Children and Young Peoples Services (in Local Authorities) |
| FOSI | Family Online Safety Institute |
| EA | Education Authority |
| ES | Education Scotland |
| GDPR | General Data Protection Regulations |
| HWB | Health and Wellbeing |
| ICO | Information Commissioners Office |
| ICT | Information and Communications Technology |
| ICTMark | Quality standard for schools provided by NAACE |
| INSET | In Service Education and Training |
| IP address | The label that identifies each computer to other computers using the IP (internet protocol) |

| | |
|---|---|
| ISP | Internet Service Provider |
| ISPA | Internet Service Providers' Association |
| IWF | Internet Watch Foundation |
| LA | Local Authority |
| LAN | Local Area Network |
| MIS | Management Information System |
| NEN | National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain. |
| Ofcom | Office of Communications (Independent communications sector regulator) |
| SWGfL | South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW |
| TUK | Think U Know – educational e-safety programmes for schools, young people and Parents/Carers. |
| VLE | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting |
| WAP | Wireless Application Protocol |