

Online Safety Policy



| | | |
|---------------------|---------------------|---------------|
| Approved by: | Full Governing Body | Date: 15.5.25 |
| Chairs of Governors | | |
| Last reviewed on: | May 2025 | |
| Next review due by: | Summer 2026 | |

Contents

| | |
|--|----|
| Contents | 1 |
| Development/Monitoring/Review of this Policy | 2 |
| Roles and Responsibilities | 3 |
| Policy Statements..... | 5 |
| Communications | 10 |
| Dealing with unsuitable/inappropriate activities | 12 |
| Responding to incidents of misuse | 14 |
| Illegal Incidents | 14 |
| Other Incidents..... | 15 |
| School actions & sanctions..... | 15 |
| Appendix | 19 |
| Pupil Acceptable Use Agreement Template – for older pupils | 20 |
| Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1) | 23 |
| Parent/Carer Acceptable Use Agreement..... | 24 |
| Record of reviewing devices/internet sites (responding to incidents of misuse)..... | 26 |
| Reporting Log | 27 |
| Glossary of Terms..... | 29 |

Development/Monitoring/Review of this Policy

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

- Headteacher
- Staff – including teachers, support staff
- Computing subject leader
- PSHE subject leader
- Governors
- Parents and carers

Schedule for Development/Monitoring/Review

| | |
|---|------------------------|
| This online safety policy was approved by the Governing Body on: | <i>10.05.23</i> |
| The implementation of this online safety policy will be monitored by the: | <i>The Headteacher</i> |
| Monitoring will take place at regular intervals: | <i>Annually</i> |
| The Governing Body will receive a report on the implementation of the online safety policy (which will include anonymous details of online safety incidents annually). | <i>Once a year</i> |
| The online 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 online safety or incidents that have taken place. The next anticipated review date will be: | <i>Summer 2024</i> |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | <i>LADO, Police</i> |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of
 - pupils
 - parents/carers
 - staff

Scope of the Policy

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

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

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor* which is combined with that of the Child Protection/Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the headteacher
- regular monitoring of online safety incident logs
- reporting to relevant the Governing Body

Headteacher and Online Safety Lead

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and the Deputy Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse”).
- *The Headteacher is responsible for ensuring that all staff receive suitable training to enable them to carry out their online safety roles, as relevant.*
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs
- attends relevant meetings of *Governors*

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current *school* online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the *Headteacher* for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated Safeguarding Lead

Should be trained in online 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
- online-bullying

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop).

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the pupil acceptable use agreement
- 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

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

- digital and video images taken at school events
- access to parents' sections of the website
- *their children's personal devices in the school (not permitted)*

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 online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning the online safety curriculum we refer to:

- DfE Teaching Online Safety in Schools
- NYCC guidance

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

- *A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited*
- *Key online safety messages should be reinforced as part of a planned programme of assemblies and 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.*
- *Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and approved by the headteacher.*

Education – Parents/carers

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

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

- *Curriculum activities*
- *Letters, newsletters, website*
- *Parents/carers evenings/sessions*
- *High profile events/campaigns e.g. E Safety Day*

Education & Training – Staff/Volunteers

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

- *A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.*
- *All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.*
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *This online safety policy and its updates will be presented to and discussed by staff.*
- *The Headteacher will provide advice/guidance/training to individuals as required.*

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

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

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure password by the school administrator. Users are responsible for the security of their username and password. (Group or class logons and passwords will be used for KS1 and below)
- The “master/administrator” passwords for the school systems, used by the Network Manager (or other person) are held by SchoolsICT
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users – staff/pupils etc)

- *An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).*
- The school infrastructure and individual devices are protected by up to date virus software.
- *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.***

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

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 online-bullying 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy. (This is addressed through a suite of policies)
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents and volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.

- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

The school does not allow data storage on USBs.

When personal data is stored on any mobile device the:

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

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

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 |
| Mobile phones may be brought to the school | X | | | | | | X |
| Use of mobile phones in lessons | | | | X | | | X |
| Use of mobile phones in social time (must not be in the company of children) | X | | | | | | X |
| Taking photos on mobile phones/cameras | | | | X | | | X |
| Use of other 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 blogs | | X | | | | | X |

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, social media, chat, blogs, 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.*
- *Pupils are not given email addresses, although logins for Microsoft Teams take this format.*

- *Pupils should be taught about online 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, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority/MAT 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:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|--|--|------------|-----------------------------|--------------------------|--------------|--------------------------|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges | | | | | 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 | |
| | | | | | | |

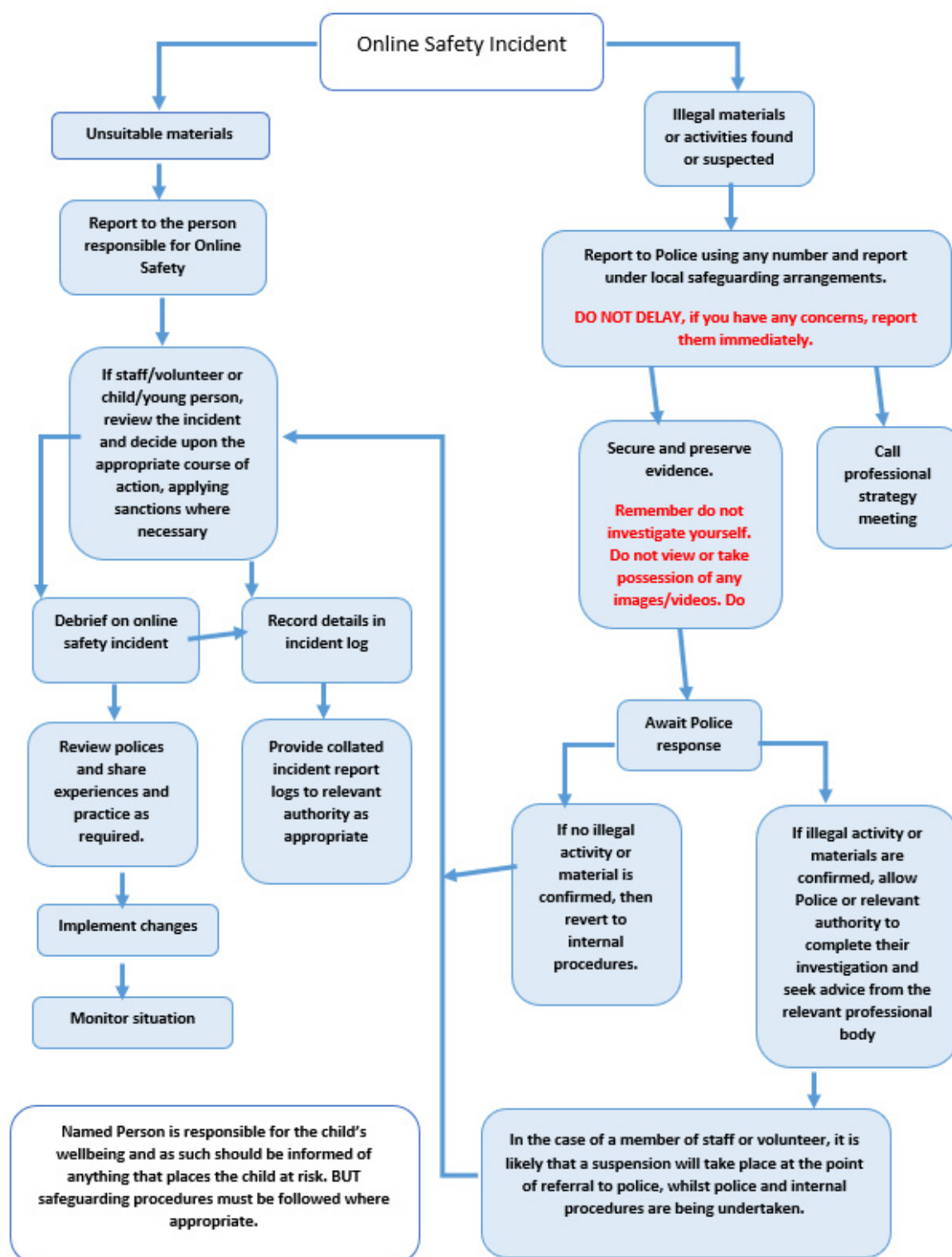
| | | | | | |
|--|---|---|---|---|---|
| Promotion of extremism or terrorism | | | | X | |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| <p>Activities that might be classed as cyber-crime under the Computer Misuse Act:</p> <ul style="list-style-type: none"> Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission) <p>The Schools will decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here</p> | | | | | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | | | | X | |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | X | |
| Using school systems to run a private business | | | | X | |
| Infringing copyright | | | | 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 | | |

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national/local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - 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 safeguarding 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/tutor | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Warning | Further sanction e.g. detention/exclusion |
|--|------------------------------|----------------------|-----------------|--|-----------------------|---|---------|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | | X | X | | | | | |
| Unauthorised use of non-educational sites during lessons | X | | | | | | | |
| Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device | X | X | | | X | | | |
| Unauthorised/inappropriate use of social media/messaging apps/personal email | X | X | | | X | | X | |
| Unauthorised downloading or uploading of files | X | X | | X | | | | |
| Allowing others to access school network by sharing username and passwords | X | X | | | X | | X | |
| Attempting to access or accessing the school network, using another student's/pupil's account | 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 | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | 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 | | | X |
| Using proxy sites or other means to subvert the school's filtering system | X | X | | X | | | X | |

| | | | | | | | |
|---|---|---|--|---|---|--|---|
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | X | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | | X | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X | | | X | | X |

| | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
|--|-----------------------------|-----------------|--|---------|------------|---------------------|
| Staff Incidents | | | | | | |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | X | X | | | X | X |
| Inappropriate personal use of the internet/social media/personal email | | | | X | | X |
| Unauthorised downloading or uploading of files | | | | X | | |
| 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 | | |
| Deliberate actions to breach data protection or network security rules | | | X | | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | | | | | X |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils | X | | | | X | X |
| Actions which could compromise the staff member's professional standing | | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | | | | | X |

| | | | | | | |
|--|---|---|---|---|---|---|
| Using proxy sites or other means to subvert the school's filtering system | | | X | | 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 |
| Breaching copyright or licensing regulations | | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | | | | | X |

Appendix

Appendices

| | |
|--|----|
| Contents | 1 |
| Development/Monitoring/Review of this Policy | 2 |
| Roles and Responsibilities | 3 |
| Policy Statements..... | 5 |
| Communications | 10 |
| Dealing with unsuitable/inappropriate activities | 12 |
| Responding to incidents of misuse | 14 |
| Illegal Incidents | 14 |
| Other Incidents..... | 15 |
| School actions & sanctions..... | 15 |
| Appendix | 19 |
| Pupil Acceptable Use Agreement Template – for older pupils | 20 |
| Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1) | 23 |
| Parent/Carer Acceptable Use Agreement..... | 24 |
| Record of reviewing devices/internet sites (responding to incidents of misuse)..... | 26 |
| Reporting Log | 27 |
| Glossary of Terms..... | 29 |

Pupil Acceptable Use Agreement Template – for older pupils

School policy

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

This acceptable use agreement 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 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 Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the 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 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 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 install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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 online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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

Pupil Acceptable Use Agreement Form

This form relates to the *pupil* acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school 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 equipment out of the school 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:

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

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

Signed (parent):

Parent/Carer Acceptable Use Agreement

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 and carers are aware of the importance of online 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 agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

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

Permission Form

Parent/Carers Name:

Pupil Name:

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

Either: (KS2 and above)

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

Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online 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 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 systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

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 online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

| |
|---|
| This form will be stored electronically on the school's management system. |
| The school administrator, headteacher and class teacher will have access to this information. |
| The form will be stored for the time the child is a pupil at the school. |
| The form will be deleted from the school system. |

Signed:

Date:

Use of Digital/Video Images

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. Where an image is publicly shared by any means, only your child's first name will be used.

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

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

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

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

Group:
Date:
Reason for investigation:
.....
.....

Details of first reviewing person

Name:
Position:
Signature:

Details of second reviewing person

Name:
Position:
Signature:

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

.....
.....

| Web site(s) address/device | Reason for concern |
|----------------------------|--------------------|
| | |
| | |
| | |

Conclusion and Action proposed or taken

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

Reporting Log

Group:

| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
|------|------|----------|--------------|----------|----------------------|-----------|
| | | | What? | By Whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Password Security

Further guidance can be found from the [National Cyber Security Centre](#) and [SWGfL "Why password security is important"](#)

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and pupils) 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.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- 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
- Passwords must not include names or any other personal information about the user that might be known by others
- *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

Learner passwords:

- Records of learner usernames and passwords for foundation phase pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for pupils at Key Stage 2 and above should increase as pupils progress through school.
- Users will be required to change their password if it is compromised.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Training/Awareness:

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

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement

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

- in lessons addressing security

- through the acceptable use agreement

Glossary of Terms

| | |
|-------------------|--|
| AUP/AUA | Acceptable Use Policy/Agreement – see templates earlier in this document |
| CEOP | Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| CPD | Continuous Professional Development |
| FOSI | Family Online Safety Institute |
| ICO | Information Commissioners Office |
| ICT | Information and Communications Technology |
| 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 |
| MAT | Multi Academy Trust |
| 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 online safety programmes for schools, young people and parents. |
| UKSIC | UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation. |
| UKCIS | UK Council for Internet Safety |
| VLE | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting, |
| WAP | Wireless Application Protocol |

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

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

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

