



E-safety Policy

Owner:	Headteacher
Approved by:	School Development Board
Last review:	September 2022
Approved:	September 2021
Next review due:	May 2025



Callowell Primary School, Barrowfield Road, Stroud, Gloucestershire, GL5 4DG
Tel: 01453 762962 email: admin@cps.cbat.academy
Part of Cotswold Beacon Academy Trust, registered in England and Wales
No. 0769339. Registered office: Cainscross Road, Stroud, GL5 4HE
registeredoffice@cbat.academy

Callowell Primary E-Safety Policy

The school monitors the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers & staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of 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. The 2014 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors

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 another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety

incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).

- The Headteacher is responsible for ensuring that the E-Safety Lead 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 ensures 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 provides a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team receive monitoring reports from the E-Safety Lead when issues arrive.

E-Safety Lead:

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

ICT Coordinator:

The Coordinator for ICT 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
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- reports sites that need filtering to the SWGFL filtering service
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

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 / E-Safety Lead for investigation / action / sanction
- all digital communications carried out using official school systems with parents / carers should be on a professional level and there is no intentional communication with pupils
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

The DSL is trained in e-safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

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

E-Safety Group

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

Members of the E-safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

Pupils have a responsibility to:

- use 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
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras.
- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

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

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

Policy Statements

Education – pupils

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

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

- A planned e-safety curriculum as part of Computing / PHSE / other lessons is regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are helped to understand the need for the pupil Acceptable Use of Technology Policy and are encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, pupils are 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 are vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Parents 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 option including:

- Curriculum activities
- Letters, newsletters, web site, DoJo
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

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

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school's online presence provide e-safety information for the wider community

Education & Training – Staff

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal e-safety training is available to staff. This is regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly by the E Safety Group.
- All new staff 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 (or other nominated person) receives regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) or reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) provides advice / guidance to individuals as required.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor but it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. The managed service provider is fully aware of the school E-Safety Policy / Acceptable Use of Technology Policy. The school also checks their Local Authority / other relevant body policies on these technical issues.

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

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school technical systems
- All users have clearly defined access rights to school technical systems and devices.
- The “administrator” password for the school ICT system, used by the ICT Co-Ordinator must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The ICT Coordinator 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.
- Any actual / potential technical incident / security breach must be reported to the ICT Coordinator / Head.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- A temporary login for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) is available and the password is regularly changed to prevent unauthorised access onto the school systems.
- Only a member of staff is allowed to use school devices outside of school. The limits of use of school devices is set out in the Acceptable Use of Technology Policy.

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. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- The school's expectations and responsibilities for all users is set out in the Acceptable Use of Technology Policy.
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory e-safety training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Any device loss, theft, change of ownership of the device will be reported
- Any user leaving the school will follow the process outlined

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 inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular the children recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (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.
- 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 in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

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

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

The school must ensure that:

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices wherever possible.

Where possible and practical, personal data stored on any portable computer system, memory stick or any other removable media be:

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

Should this not be practical or possible, the user takes responsibility for issues arising from the data being lost or misused.

Communications

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

Staff and other adults are permitted to bring mobile devices into school and appropriate use is permitted at relevant times. Any data, information or photos/videos is available for inspection by other members of staff on request.

Pupils may bring mobile devices into school but they must remain turned off during the school day and placed in a safe place by the child’s class teacher. The teacher and school cannot be held responsible for any items lost or damaged.

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 are aware that email communications are monitored.
- 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 parents / carers in an official capacity (email, Class Dojo, VLE etc) must be professional in tone and content.
- pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 includes: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff ensure that:

- No reference is 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 is checked regularly by the senior risk officer and e-safety committee to ensure compliance with the other school 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:

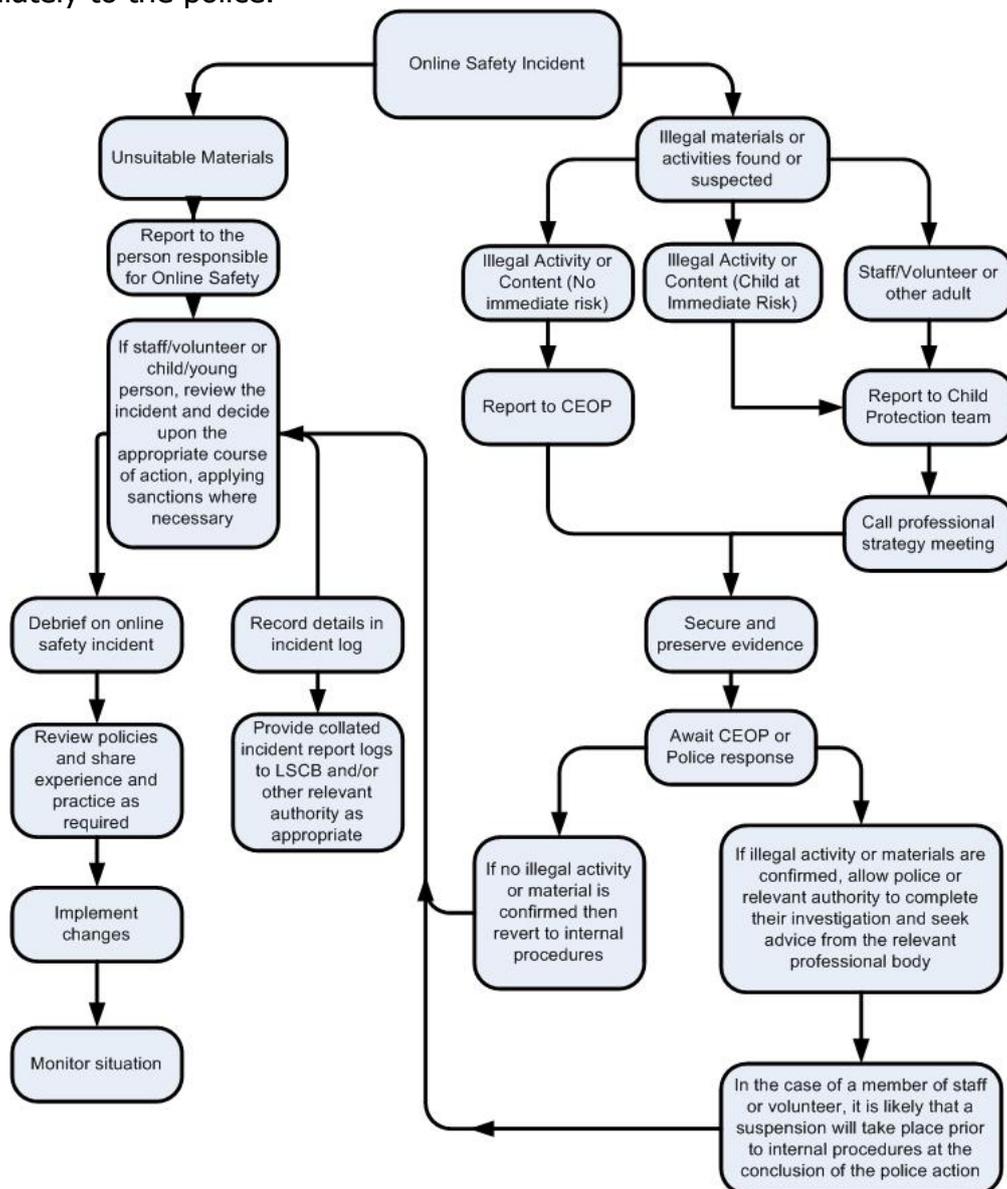
		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production 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				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			X		
On-line gaming (educational)			X		
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 eg 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.

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 for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

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

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

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil Incidents:	Refer to class teacher	Refer to ICT Coordinator	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
Deliberately accessing or trying to access material that could be considered illegal (see previous list)		X	X	X		X	X	X	X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X	X		
Unauthorised use of social media / messaging apps / 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			X			X		X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X		X	X
Corrupting or destroying the data of other users	X								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X		X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X			X		X	X
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	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X						

Staff Incidents:	Refer to Headteacher	Refer to Local Authority	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				
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	X		
Careless use of personal data eg 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		
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		
Actions which could compromise the staff member's professional standing	X				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			X	X	

Appendix

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

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

Policy agreed and approved September 2021

Reviewed September 2022

Signed:(Chair Of Governors) Date