



Dream Big. Aim High
& Make a Difference

Potley Hill Primary School

Online Safety Policy

Contents

Introduction

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities

- Governors
- Headteacher and Senior Leaders
- The Designated Safeguarding Leader
- Computing Subject Leader
- IT External Company
- Information Asset Owners
- Teaching and Support Staff
- Curriculum & School Improvement Committee
- Pupils
- Parents / Carers

Policy Statements

- Education – Pupils
- Education – Parents / Carers
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Mobile Technologies (including BYOD/BYOT)
- Use of digital and video images
- Data security
- Communications
- Social Media - Protecting Professional Identity
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse
- Illegal and other Incidents
- School Actions and Sanctions

Potley Hill Online Safety Policy

Introduction

At Potley Hill Primary School we are required to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely. It is addressed as part of the wider duty of care to which all who work in schools are bound. This school will ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside of school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies

This policy should be read in conjunction with the appropriate sections of the Safeguarding Policy.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body:	23 rd March 2023
The implementation of this Online Safety policy will be monitored by the:	Governing Board
Monitoring will take place with the use of a risk assessment and safety incidents at regular intervals:	Once per year
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:	March 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LADO

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 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

Online Safety is recognised as an essential aspect of strategic leadership in Potley Hill Primary school. All teaching and support staff have received Online Safety training and are responsible for promoting and supporting safe behaviours in their classrooms following school Online Safety procedures. Overall, responsibility for Online Safety rests with the Headteacher and Governing Board, all procedures outlined in this policy assume a designation of named staff in the following roles:

Governing Board:

Governors are responsible for the approval of the Online Safety policy and for reviewing its effectiveness, including the monitoring of the policy, the impact of initiatives and any changes of recurring events e.g. filtering changes.

Potley Hill Online Safety Policy

Headteacher:

The Headteacher is the Responsible Manager of the school for all Health and Safety aspects, this includes Online Safety for pupils, staff and visitors. Although the day to day responsibility for online safety will be delegated to the Computing Subject Leader, the Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious 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” and relevant HCC disciplinary procedures).

The Headteacher is responsible for ensuring that the Computing Subject Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Furthermore, the Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Designated Safeguarding Lead:

Designated Safeguarding leads (DSL) 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
- cyber-bullying

DSLs should be made aware of any Online Safety issues and have access to the record of behaviour or safeguarding concern recordings. As well as this, DSLs should be made a part of the review team which looks at the policy should any changes need to be made. Training and advice for staff should be offered to ensure that the correct procedures are always followed in the event of an online safety incident taking place, this includes liaising with the local authority or other relevant bodies and attending any relevant governors’ meetings.

Computing Subject Leader & IT External Company:

The Computing Subject Leader and the school’s external IT Company are responsible for ensuring that the school’s technical infrastructure is secure and is not open to misuse or malicious attack. They also need to certify that the school meets required online safety technical requirements and any Local Authority online Safety Policy and guidance that may apply. With regards to network access, they need to continue to ensure that users may only access the networks and devices through a properly enforced password protection policy. Also, system and data backups are carried out daily and checked for validity at least once a term.

Information Asset Owners:

These are people who compile specific information and their role is to be clear about:

- what information they hold, and for what purpose
- how this information will be amended or added to over time
- who has access to the information and why
- how information is retained and disposed of

Teaching and Support Staff:

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. All staff must read, understand and sign the Staff Acceptable Use Policy (AUP). Any misuse of the equipment or online resources must be reported to the headteacher, DSL or Computing Subject Leader for investigation. All digital

Potley Hill Online Safety Policy

communications with pupils, parents or carers should be on a professional level and only carried out using official school systems.

Pupils:

Pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, information evenings, curriculum activities and safety campaign 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 and access to parents' sections of the website and any pupil records.

Policy Statements - Full policies where applicable can be accessed through the website or from the school office

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 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.

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 should be provided as part of Computing, PDL or other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities
- Pupils should be taught in all lessons to be critically aware of the materials and 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.

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 and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, bulletins, web site
- Parents' and carers' evening sessions
- High profile events and campaigns e.g. Safer Internet Day

Education – The Wider Community:

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.

Potley Hill Online Safety Policy

- The school website will provide online safety information for the wider community
- CEOP training sessions for parents of the community linked with other schools in the community.

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:

- 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.

Training – Governors:

Governors should take part in online safety awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation
- Participation in school training and information sessions for staff or parents
- Via online training platforms provided by NGA etc.

Technical – infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible. Policies and procedures approved within this policy will be 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:

- The School has the responsibility to ensure all technical security is implemented and managed in ways that ensure that the school meets recommended technical requirements from the government and local authority.
- 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 will be provided with a username and secure password. Users are responsible for the security of their username and password.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- A backup policy is in place and regular restores of this data is carried out to test the validity of the backups
- Internet access is filtered for all users.
- Users are made aware that their activity is monitored in the Acceptable Use Agreement.
- A user can report any actual or potential technical incident and security breach to the Computing Subject Leader who will liaise with the Headteacher (and designated safeguarding leader).
- The school infrastructure and individual workstations are protected by up to date virus software.
- There is provision for temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems via a restricted log-on.
- Staff and their family members are able to use school devices, such as laptops, out of school though acceptable use guidelines should be followed at all time and laptops should not be used to store personal information or photographs.

Mobile Technologies (including BYOD/BYOT)

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 the school’s learning platform and other cloud based services such as email and data storage.

Potley Hill Online Safety Policy

All users should understand that the primary purpose of the use mobile or personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

****Only school devices will have full network access any personal devices will not be allowed to connect to the school network or WI-FI.***

Currently, the school does not operate a BYOD system. This will be reviewed periodically.

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.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In line with our GDPR policy, we no longer allow parents/carers to take videos and digital images of their children at school events. To respect everyone's privacy and in some cases protection, parents/carers are now reminded regularly that this is not permitted.

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)

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.

Potley Hill Online Safety Policy

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

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

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

Data Security

Backups are intended to provide protection for all your data. Schools need to be able to restore their data in the event of:

- Accidental deletions
- Application errors
- Hardware and or system failure
- Disaster at the school (fire, theft, flood....)
- Malicious attacks such as viruses

All data held on centrally held school systems is automatically backed up at the end of each day. Staff should access pupil information (such as reports, tracking information) via remote access to the central system and avoid copying this personal information onto removable devices.

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 or disadvantages:

Potley Hill Online Safety Policy

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be 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 pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

Social Media - Protecting Professional Identity

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

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

- Ensuring that personal information is not published
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority

Potley Hill Online Safety Policy

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Personal communications are those made via a personal social media accounts. 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
- 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's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the appropriate 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	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions 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	
	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		
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		

Potley Hill Online Safety Policy

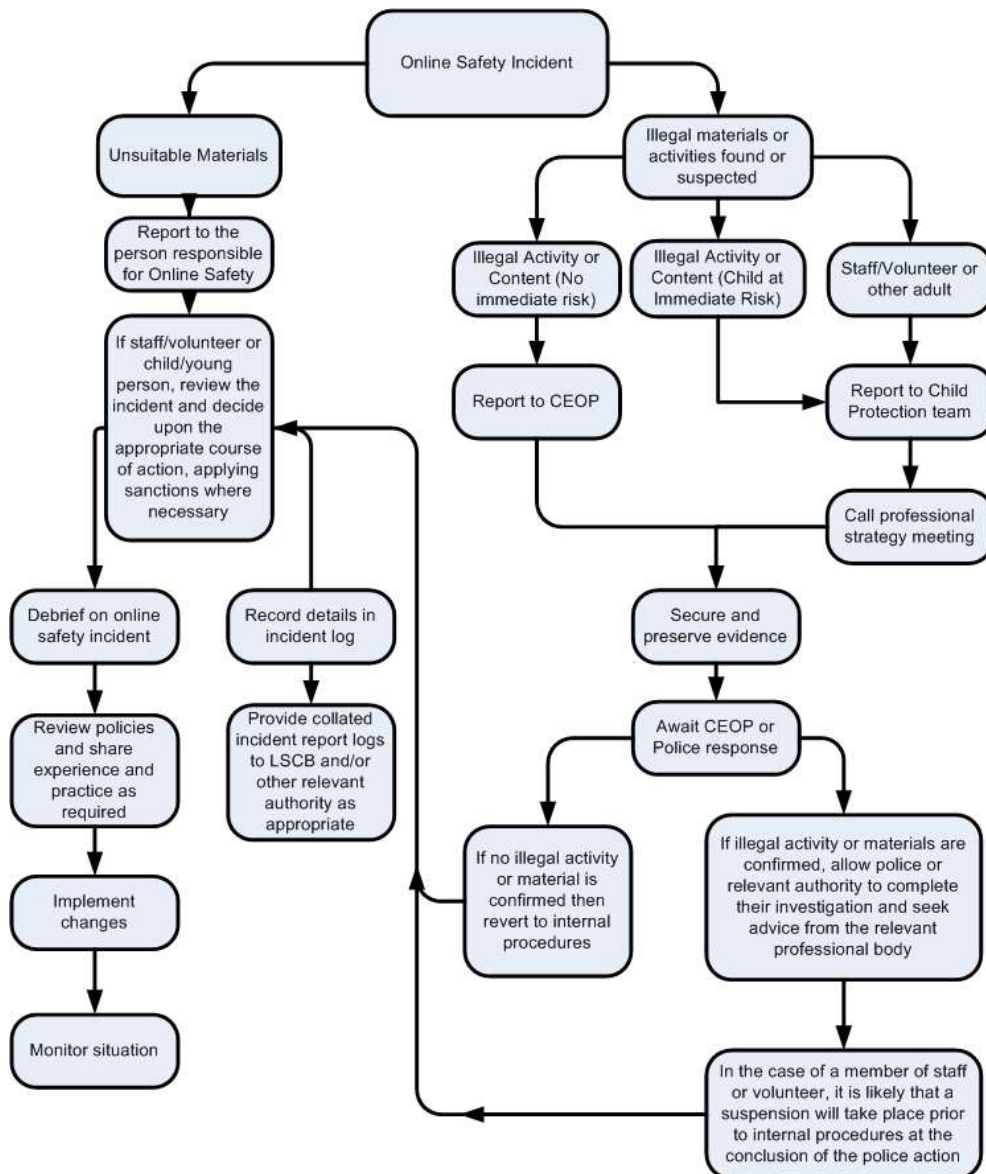
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube	X				

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



Potley Hill Online Safety Policy

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 - LADO
 - 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 or disciplinary procedures as follows:

Potley Hill Online Safety Policy

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Team Leader	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X		X			
Unauthorised use of non-educational sites during lessons	X		X			X			
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X			
Unauthorised use of social media / messaging apps / personal email	X		X			X			
Unauthorised downloading or uploading of files		X	X		X	X	X		
Allowing others to access school network by sharing username and passwords			X		X	X	X		X
Attempting to access or accessing the school network, using another student's / pupil's account			X		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		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X		X	X	X	X
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 / academy'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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X	X	X

Potley Hill Online Safety Policy

Staff

Incidents:	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X				X		X
Unauthorised downloading or uploading of files	X				X		
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 eg holding or transferring data in an insecure manner	X						X
Deliberate actions to breach data protection or network security rules	X	X	X			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			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X				X	X
Actions which could compromise the staff member's professional standing	X	X				X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	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
Breaching copyright or licensing regulations	X				X		X
Continued infringements of the above, following previous warnings or sanctions	X						X

Reviewed: March 2023
Next Review: March 2024

Potley Hill Online Safety Policy

Appendices

- A. Acceptable Use Policy
- B. Staff and Volunteers Acceptable Use Agreement
- C. Technical Security Policy
- D. Social Media Policy
- E. Mobile Technologies Policy

Related Policies

- Behaviour
- Anti-Bullying
- Child Protection
- Safeguarding
- Computing
- Equalities
- Inclusion
- Teaching & Learning
- Data Protection
- Privacy Notice

A. Acceptable Use 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 internet access at all times.

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

B. Acceptable Use Policy Agreement for staff, volunteers and governors

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. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities, this includes unprofessional behaviour when using social media sites or those which are open to the public for example YouTube.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use most importantly that personal electric equipment cannot be connected to the school's network or WI-FI.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted; or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Potley Hill Online Safety Policy

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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

Staff / Governor/Volunteer Name:

Signed:

Date:

C. TECHNICAL SECURITY POLICY (including filtering and passwords)

Introduction

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

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

Responsibilities

The management of technical security will be the responsibility of the Headteacher, Computing Subject Leader, External IT Company and Senior Administrative Officer

Technical Security

Policy statements

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

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- All users will have clearly defined access rights to school technical systems.

Potley Hill Online Safety Policy

- Users will be made responsible for the security of their username and password and 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
- The External IT company is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place
- School technical staff, regularly monitor and record the activity of users on the school technical systems by using the FWF reporter tool and users are made aware of this in the Acceptable Use Agreement.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- The Senior Administrative Officer is responsible for users (staff / pupils / community users) and their family members access to school devices that may be used out of school.
- The Senior Administrative Officer manages the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username and password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Curriculum and School Improvement Committee.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The administrator passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe.
- All users (adults and young people) will have responsibility for the security of their username and password. They 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 for new users, and replacement passwords for existing users will be allocated by the IT Manager*

Staff Passwords

- All staff users will be provided with a username and password for logging onto the school system.

Potley Hill Online Safety Policy

- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- *must not include full names or any other personal information about the user that might be known by others*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*

Student / Pupil Passwords

- All users are provided with a username which is their first initial and surname
- Pupils will be taught the importance of only logging into their own area and using the school network correctly
- The complexity (i.e. minimum standards) of the username has been set based on the cognitive ability of the children.

Training / Awareness

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

- at induction
- through the school's 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
- through the Acceptable Use Agreement

Filtering

Introduction

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

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Head Teacher, Senior Administrative Officer and Computing Subject Leader. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists.

Potley Hill Online Safety Policy

The schools filtering policy will be managed in line with this policy and all users have a responsibility to report immediately to the Headteacher, Computing Subject Leader or the Senior Administrative Officer any infringements of the school's filtering policy of which they become aware of or any sites that are accessed, which they believe should have been filtered.

To ensure that there is a system of checks to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person prior to changes being made
- be updated every 12 weeks in the form of an audit of the change control logs
- be reported to the Curriculum & School Improvement Committee half termly

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through:

- the online safety education programme.
- Warnings will also be given with regards to the consequences of attempting to subvert the filtering system.

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

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

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement, online safety awareness sessions and the newsletter.

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

D. SOCIAL MEDIA POLICY

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Potley Hill recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. 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.

Organisational control

Roles & Responsibilities

- **SLT**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.

Potley Hill Online Safety Policy

- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

- **Administrator / Moderator**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school accounts
 - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

Potley Hill Online Safety Policy

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users and their comments or posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

Potley Hill Online Safety Policy

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
 - Personal communications are those made via a personal social media accounts. 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.*
- **Pupils**
 - Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
 - The school's education programme should enable the pupils to be safe and responsible users of social media.
 - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
 - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
 - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- 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.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Potley Hill Online Safety Policy

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances