

2024- 2025

Peel Hall Primary School
Head Teacher – S Lawler-Smith



PEEL HALL PRIMARY SCHOOL

ONLINE SAFETY AND MOBILE TECHNOLOGY POLICY

Online Safety and Mobile Technology Policy

Peel Hall Primary School

Head Teacher: S. Lawler-Smith

Named personnel with designated responsibility

Designated SLT	Deputy designated SLT	Nominated Governor	Chair of Governors
S. Lawler-Smith D. Howarth	C.Wilson	H.Aaron	H.Aaron

Head Teacher	Sign and Date	
Chair of Governing Board	Sign and Date	

Next Review Date	September 2025
Committee Responsible	Governing Board
Document locations	Shared Drive

Change History

Version	Date	Change Description	Stored
1	Sept 2024	Introduction of policy	Staff Drive

This policy should always be read in conjunction with the School's Safeguarding and Child Protection Policy and the most recent version of Keeping Children Safe in Education

Scope of the Policy

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

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safety and Mobile Technology Policy and for reviewing the effectiveness of the policy.

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Head Teacher and another member of the Senior Leadership Team/Senior Management 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.
- The Head Teacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher 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.

Online Safety Coordinator/Officer:

At Peel Hall, this role is taken by Emily Grayshon and Jack Newby who:

- Take day-to-day responsibility for online safety issues within their respective phases and has a leading role in establishing and reviewing the school Online Safety and Mobile Technology Policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports regularly to the Senior Leadership Team.

Network Manager / Technical staff:

The Managed Service provider (RM) is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the online safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- The use of the network/internet/remote access/email is regularly monitored so that any misuse or attempted misuse can be reported to the Head Teacher or Online Safety Co-ordinator.

Appropriate filtering for Education Settings

Our Safeguarding responsibilities in regards to 'Appropriate' Filtering and Monitoring are supported by RM and SCC. It is important to recognise that no filtering systems can be 100% efficient and need to be supported with good teaching and learning practice and effective supervision.

RM, as filtering providers, ensure that access to illegal content is blocked by

- being IWF members
- blocking access to illegal images by actively implementing the IWF CAIC list
- integrating the 'police assessed list of unlawful terrorist content on behalf of the Home Office' Full details can be found at RM Provider Checklist Responses Please also see our Filtering Policy (RM).

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 and Mobile Technology Policy and practices.
- They have read, understood and signed the school Acceptable Use Policy Agreement (AUP).
- They report any suspected misuse or problem to the Phase Leader for their phase or the Deputy Head Teacher for their phases for investigation/action/sanction.
- They ensure online safety issues are embedded in all aspects of the curriculum.

Designated person for child protection/safeguarding

is trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Pupils *should*:

- Use the school ICT systems and mobile technologies in accordance with the advice posters on display in each classroom.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practices when using digital technologies out of school.

Parents/Carers

Parents and carers will be encouraged to support the school in promoting good online safety practice at school and at home and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- The comments section on the school **app**.
- Their children's personal devices in school (where this is allowed).

Guest Users

Guest Users (E.g. trainee teachers, supply teachers) who wish to access school ICT systems will be notified of and expected to agree to the Acceptable Use Policy Agreement before being provided with access to school systems.

Online Safety Education and Training

Education – Pupils

While 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 education will be provided in the following ways:

- A planned online safety programme will be provided as part of Computing/PHSE/other lessons and will be regularly revisited. This will cover both the use of technologies in and outside school and will include information about the risks of online gambling in 'Apps' and in online games.
- Key online safety messages will be reinforced as part of a planned programme of assemblies.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff.
- An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety and Mobile Technology Policy and Acceptable Use Policies.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for the Governor responsible for technology / online safety / health and safety / child protection. This may be offered in a number of ways:

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

Information to parents/guardians

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

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

- Letters / newsletters / school website.
- Parents' information evenings.
- National events. E.g. Safer Internet Day.
- Useful links to CEOP's website www.thinkuknow.co.uk

Use of digital and video images

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. For example, on sites and in apps such as Facebook, Twitter, Instagram and Snapchat.

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 students/pupils in the digital/video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is in compliance with the Data Protection Act 2018.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 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 no more than 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 2018 (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 safekeeping 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.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows our policy on the use of these devices and methods in school. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students / Pupils			
	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Communication Technologies								
Mobile phones may be brought to school		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		
Use of mobile phones in lessons or when supervising pupils	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>			
Use of mobile phones in social time		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			
Taking photos on mobile phones / cameras (unless it is a school owned device)	<input checked="" type="checkbox"/>							
Use of other mobile devices eg tablets, gaming devices (school devices only)		<input checked="" type="checkbox"/>						
Use of personal email addresses in school, or on school network					<input checked="" type="checkbox"/>			
Use of school email for personal emails	<input checked="" type="checkbox"/>							
Use of messaging apps					<input checked="" type="checkbox"/>			
Use of social media					<input checked="" type="checkbox"/>			



This table indicates when some of the methods or devices above may be allowed:

Communication method or device	Circumstances when these may be allowed	
	Staff & other adults	Students/Pupils
Mobile phones may be brought to school		To be handed in to the office at the start of the day and collected at home time. Only to be used on school premises with the permission of a member of staff and only in certain circumstances. E.g. to get a contact number or other relevant detail, to ring a parent/carer (teacher to be present for this).
Use of mobile phones in lessons		
Taking photos on personal mobile phones or other camera devices	Only use own devices with permission from member of SLT when a school device isn't available to use.	
Use of personal email addresses in school, or on school network	During breaks, lunchtimes or other non-contact time.	
Use of social media	During breaks, lunchtimes or other non-contact time.	

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

- Users must immediately report, to the nominated person – in accordance with the school / academy 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 communication from staff to parents / carers by email must be professional in tone and content. These communications may only take place via school email address. Personal email addresses, text messaging or social media must not be used for these communications.

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.

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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff must not accept friend or follower requests from past or present pupils unless related. E.g. son, daughter, nephew, niece etc.
- Staff should not accept friend or follower requests from parents/carers. The exception to this is where there is already a social relationship in place.
- In any conversation on social media, staff should uphold high professional standards.

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” below).

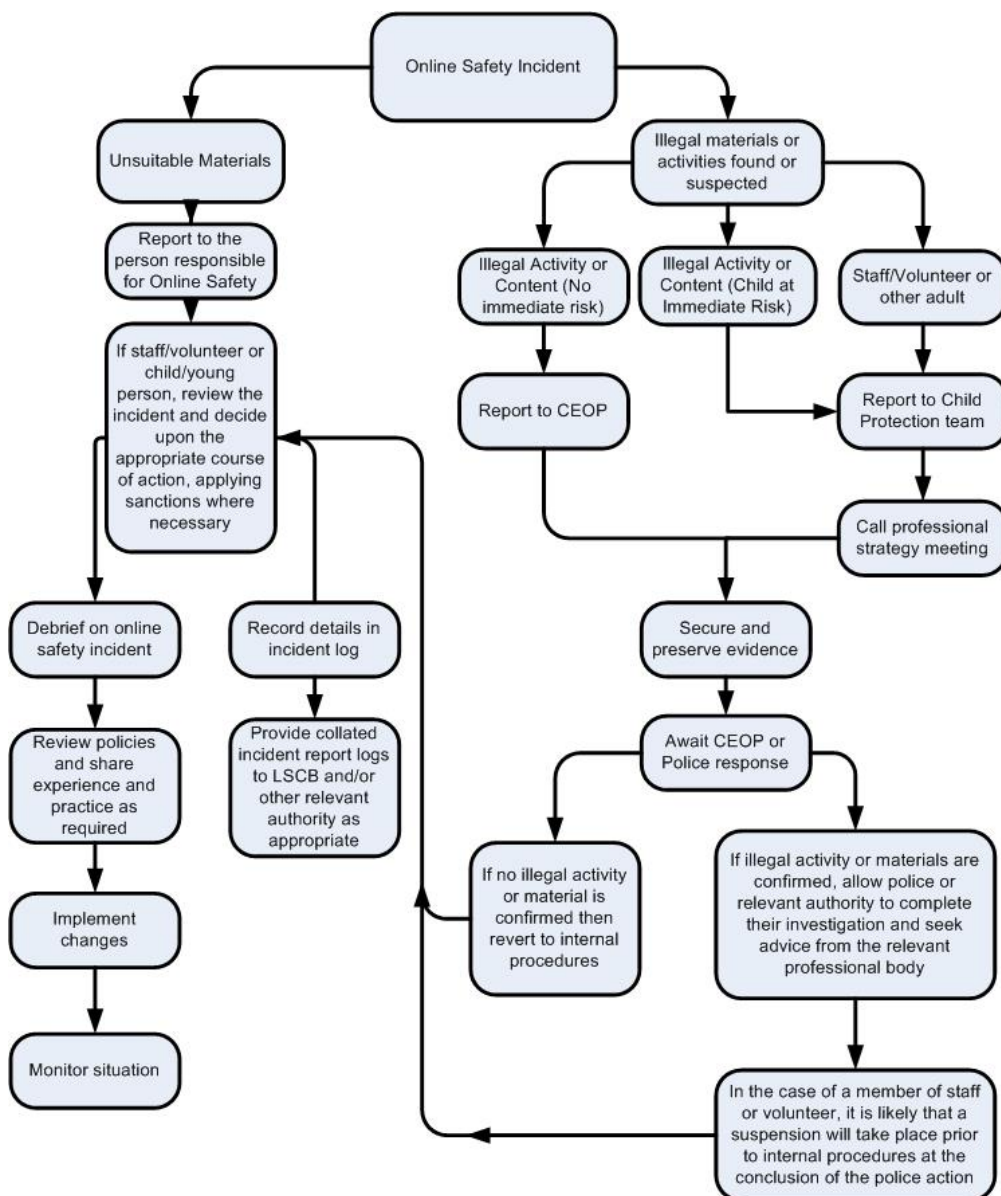
Unsuitable/inappropriate activities

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 certain internet 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:					X
	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	

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



Other Incidents

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

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

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

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

School Actions & Sanctions

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

Pupils

Incidents:	Refer to class teacher	Refer to HT or member of SLT	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 list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	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				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users		X		X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident.		X		X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X			X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Incidents:	Refer to line manager	Refer to Head Teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Further Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X				X	
Unauthorised downloading or uploading of files	X				X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X	
Deliberate actions to breach data protection or network security rules		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 students / pupils		X	X				X
Actions which could compromise the staff member's professional standing		X	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
Breaching copyright or licensing regulations		X					X
Continued infringements of the above, following previous warnings or sanctions		X					X

Further information and support

For a glossary of terms used in this document:

<http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf>

For online safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

<http://www.salford.gov.uk/d/online-safety-Practice-Guidance.pdf>

R u cyber safe?

Online safety tips about how to stay safe online:

<http://www.salford.gov.uk/rucybersafe.htm>

Appendix 1 – Staff Acceptable Use Policy Agreement

The rules set out in this agreement relate to:

- the use of school ICT systems and devices; personal ICT devices and digital communication.
- the use of all of the above in and out of school.

For my personal and professional safety, when using school ICT systems:

- I understand that the school will monitor my use of the school's ICT systems and emails.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- 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, it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate digitally with parents/carers using SeeSaw, official school emails or the school text messaging service.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's Online Safety and Mobile Technology Policy set by the school about such use.
- I will not try to upload, download or access any materials which are illegal, 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 only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Act 2018.

When using social media:

- Do not make any named or negative references about any member of the school community.
- Do not engage in online discussion on personal matters relating to members of the school community.
- Do not attribute personal opinions to the *school* or local authority.
- Regularly check security settings on personal social media profiles to minimise risk.
- Do not accept friend or follower requests from past or present pupils unless related (E.g. son, daughter, nephew, niece etc.) or there is an existing social relationship with their parents.
- Do not accept friend or follower requests from parents/carers unless there is an existing social relationship in place.
- Uphold high professional standards.

I have read and understood the rules in this agreement along with the online Safety and Mobile Technology policy before signing below.

NAME: _____ POSITION: _____

SIGNED: _____ DATE: _____

Appendix 2 – Pupil's AUP

Pupil User Acceptable Use of ICT Agreement

September 2024

- I understand that I am responsible for my actions in and out of school.
- I agree to be kind and considerate online in and out of school.
- I will behave in a responsible way online in and out of school.
- I will not post photos of people online without their permission.
- I will respect all ICT equipment in school, such as iPads, laptops and Chromebooks, treating them with care.
- If I see something online that worries me, I will tell a trusted grown-up straight away. If this happens in school, I will tell a teacher or teaching assistant.
- My school will monitor my use of ICT. This means my teachers can see which websites I have been on.
- I understand that the laptops/iPads/Chromebooks in school are to help me with my school work.
- I will not share my password with anyone else.
- I will not try to use anyone else's username and password.

Signed:

Full name:

Class:

Appendix 3 – Children’s AUP (EYFS – children not required to sign)

Pupil User Acceptable Use of ICT Agreement

September 2024

EYFS

I will take care of the laptops and iPads in my classroom.

If I see something online that upsets me, I will tell a grown-up.

I will be kind online.

Laptops and iPads in school help me with my learning.