PERRYFIELDS INFANT SCHOOL

Helping each other to learn and grow

INTERNET USE AND ONLINE SAFETY POLICY

Approved By	Date	Next Review Date
LGB	28th November 2022	Autumn Term 2023

Perryfields Infant School

Internet Use and Online Safety Policy

Perryfields Infant School
Internet Use and Online Safety Policy

Introduction

The internet is now an essential part of modern life and the school has a duty to provide children with quality internet access as part of their learning, as well as access to other digital technologies. It also has a duty to help them to develop the necessary skills to use technology safely and to know what to do if they encounter something worrying online.

The internet in our computing curriculum

As part of our computing curriculum, children will learn to use email and blogs via our learning platform, for which each child is provided with their own username and password. They will also access various online resources to learn simple coding, to create pictures, graphs and databases, and they will learn to carry out searches on the internet using a search engine, as well as accessing online educational games.

Because the internet runs through all our blocks of learning, e-safety forms an integral part of each block. Children will be taught to alert an adult if they see anything online that worries them or if they receive an offensive email. They will learn not to reveal personal details or their passwords.

Learning from home

From time to time it may be necessary for children to learn from home, accessing resources set by their teachers on the school website or on DBPrimary, the school's learning platform. Full information about learning from home is included in the school's Remote Learning Policy.

As the internet is now integral to all our lives, the body of this policy sets out the measures used by Perryfields Infant School to keep all members of the school community safe when using it, whether at home or at school.

Scope of this policy

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

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Perryfields Infant School. The term “regular” means at least once a term.

Local Governing Body (LGB) Governors:

LGB Governors are responsible for the adoption of the Online Safety Policy and monitoring its effectiveness. In order to do this, they will receive regular information about online safety incidents. The member of the LGB who is the Safeguarding Governor will additionally take on the role of Online Safety Governor. This role will include:

- Regular meetings with the Online Safety Co-ordinator
- Regular monitoring of online safety incident logs
- Reporting to the LGB and, if required, the Board of the Chelmsford Learning Partnership.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and other members 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.
- The Headteacher is responsible for ensuring that the Online Safety Co-ordinator 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 Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out internal online safety monitoring roles.
- The Senior Leadership Team (SLT) will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Co-ordinator:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the LGB as necessary.
- Liaises with school technical support staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering.
- Reports regularly to SLT.
- Reports to the LGB, as part of the role as Computing Lead.
- Ensures they keep up to date with online safety technical information in order to carry out their online safety role effectively, and the inform and update others as relevant.

Network Manager:

Is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements.
- That users may only access the networks through a properly-enforced password protections policy.
- That the filtering policy is applied and updated regularly and that its implementation is not the responsibility of a single person.
- That the use of the network/ internet/ DBPrimary (the school's online platform)/ remote access/ email is regularly monitored in order that any misuse/ attempted misuse can be reported to the Online Safety Co-ordinator for investigation.
- That monitoring systems are implemented and updated as agreed in school policies
- That the school's Online Safety Co-ordinator is updated with regular reports on the school systems.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the school's Code of Conduct as set out in the Staff Handbook.
- They report any suspected misuse or problem to the Online Safety Co-ordinator for investigation.
- All digital communications with pupils/ parents / carers should be on a professional level and only carried out on official school systems.
- Online safety issues are embedded in all aspects of the curriculum.
- Pupils understand and follow the online safety and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found on internet searches.

Designated Safeguarding Leads

Must be trained in online safety issues and be aware of the potential for serious child protections/ safeguarding issues to arise from:

- The sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate online contact with adults/ strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

- Are responsible for using the school digital technology systems and learning platform in accordance with Responsible Use of the Internet Guidelines, which are shared with pupils regularly as part of the computing lessons.
- Have a good, age-appropriate understanding of research skills and copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand appropriate use of digital cameras and mobile devices.
- Understand the importance of adopting good online safety practices when using digital technologies out of school.

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 newsletters, the school website, parent information evenings and information about national/ local online safety campaigns/ literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parent sections of the school website
- Their child's DBPrimary login
- Social media platforms relating to the school.

Policy Statements

Education and Training

Pupils

While technical protections are important, pupils must be educated to take a responsible approach. The education of pupils in online safety is an essential part of the school's online safety provision: children need to learn to recognise and avoid online safety risks and build their resilience to cope if they encounter them.

Staff should reinforce online safety messages across all areas of the curriculum. The online safety curriculum will be provided in the following ways:

- As part of the Computing and PSHE (including RSE) blocks of lessons.
- As part of a planned programme of assemblies and class circle times.
- As part of research in other subjects, children should be taught to be critically aware that material accessed online can be wrong and to validate accuracy. They should also be taught to acknowledge the source of information (eg. name of website) from which they access information, as an introduction to copyright.
- Pupils should be helped to understand the need for responsible use of the internet when using DBPrimary, both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- By guiding pupils to sites checked as suitable where internet use is pre-planned, but by ensuring that pupils know what to do if they find unsuitable material during internet searches.
- Where pupils are allowed free use of the internet (such as in computing clubs and Peardrops), staff should be vigilant in monitoring the content of the websites visited.

Parents/ carers

Many parents and carers have only a limited understanding of online safety risks and issues, despite playing an essential role in the education of their children and monitoring/ regulating their online behaviour. Parents and carers may underestimate how often children encounter potentially harmful or inappropriate material on the internet and may be unsure how to respond.

Perryfields Infant School seeks to address parental understanding by providing information in the following ways:

- Letters and newsletters
- Curriculum information
- The school website
- High profile events and campaigns
- Information evenings run by experienced external providers.

The wider community

- Perryfields Infant School liaises with Perryfields Junior School to ensure that advice to co-ordinated advice and approaches are used.
- Visitors to the school who are using technologies (eg. internet for assemblies) are provided with and sign to accept the Code of Conduct for using technology.

Staff and volunteers

It is essential that staff and volunteers receive online safety training and understand their responsibilities as outlined in this policy. The following training will be offered:

- Formal online safety training is made available on Flick Learning and should be completed by all staff.
- All new staff MUST receive online safety training as part of their induction, ensuring they fully understand the school online safety policy and Code of Conduct.
- All new parent helpers/ volunteers MUST receive online safety training as part of their induction, ensuring they fully understand the school online safety policy and Code of Conduct.
- The Online Safety Co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant external agencies (e.g. CEOP)
- Online Safety Policy will be presented to and discussed by staff at staff meetings and at relevant INSET days (e.g.Safeguarding update).
- The Online Safety Co-ordinator will provide advice, guidance and training to individuals as required.

LGB Governors

LGB Governors should take part in online safety training and awareness, particularly those responsible for technology/ online safety/ health and safety/ child protection. This will be offered through:

- Training by Local Authority/ National Governors Association/ other relevant organisation.
- Training by school/ information sessions for staff or parents.

Technical

Infrastructure, filtering and monitoring

The school is responsible for ensuring that the infrastructure/ network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented.

It also needs to ensure that the various people named in the sections above will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school systems.
- Servers, wireless systems and cables must be securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Head teacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by the Network Manager (or other nominated person) must also be available to the Headteacher.
- The school is responsible for ensuring that the software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (including child sexual abuse images) is filtered by the broadband or filtering provider.
- Content lists are regularly updated and monitored.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems or data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed procedure is in place for the provision of temporary access for “Guests” onto the school systems (e.g. supply teachers, student teachers, visitors).
- The Code of Conduct sets out the extent of personal use that users are allowed on school devices, including those that may be used outside school (such as laptop computers).
- An agreed policy is in place regarding the use of removable media (such as memory sticks).

Use of digital and video images

Staff, parents/ carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may lead to cyber bullying taking place. They may also remain on the internet forever, causing harm or embarrassment over a long period of time. It is common for employers to carry out internet searches for potential and existing employees. In order to educate and reduce likelihood of potential harm:

- Staff will seek to educate parents at information events, about the risks associated with taking, using, sharing, distributing and publishing images, particularly on social media sites.
- Child-friendly resources (such as those provided for the age-group by CEOP and on DBPrimary) will be used as part of the computing curriculum to introduce children to the concept that care should be taken with images.
- In accordance with advice from the Information Commissioner’s Office, parents/ carers are welcome to take videos and digital photographs of their own children are school events for their own personal use. To respect everyone’s privacy and protection, these images should not be published on social media sites. Parents will be advised of this at the beginning of such events (concerts, assemblies, productions etc.)
- Staff 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. These images should only be taken on school equipment unless otherwise authorised but must be permanently removed immediately after use.
- Care should be taken when taking video or digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- From time to time, videos are made of whole school events, such as the Christmas Play, which are sold to parents. Written permission from parents or carers will be obtained for their children to be included in these videos.
- Pupils must not take, use, share, publish or distribute images or others without their permission.
- Pupils’ full names will not be used on a website or blog in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

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

- Processed fairly, lawfully and in a transparent manner (lawfulness, fairness and transparency)
- Collected for specified, explicit and legitimate purposes (purpose limitation)
- Adequate, relevant and limited (data minimisation)
- Accurate and up to date (accuracy)
- Kept no longer than is necessary (storage limitation)
- Stored, processed and transferred with integrity and confidentiality (integrity and confidentiality)
- Processed by a controller who is accountable (accountability)

All matters regarding data protection are covered in the school's Data Protection Policies.

Social Media – protecting professional identity

Schools have a duty of care to provide a safe learning environment for pupils and staff. Schools can be held responsible, indirectly, for acts of their employees in the course of their employment: staff members who harass, cyberbully, discriminate on grounds of sex, race or disability or who defame a third party may render the school liable.

The school takes the following measures to ensure that reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

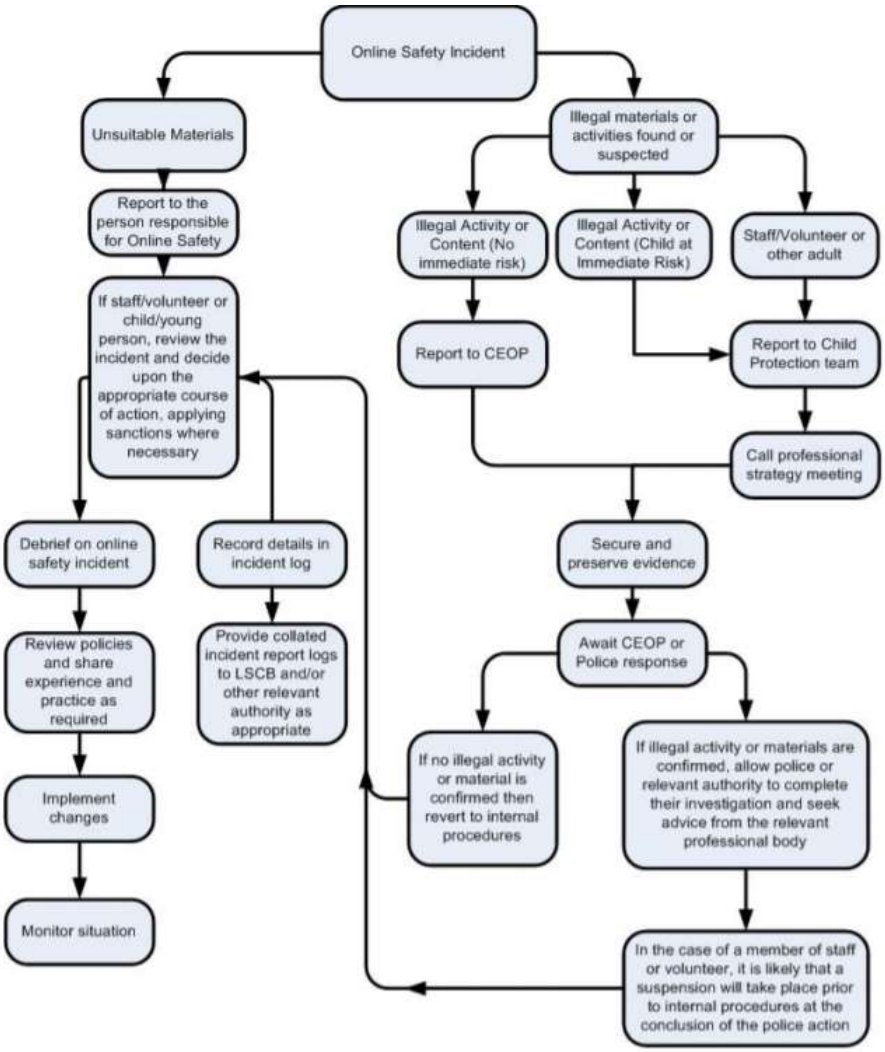
School staff should ensure that:

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

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents involving the use of online services. It encourages a safe and secure approach to the management of the incident, which may involve illegal or inappropriate activities.



Illegal incidents

If there is any suspicion that a website concerned may contain child abuse images, or if there is any other suspected illegal activity, take steps identified in the right-hand side of the flowchart above (responding to Online Safety Incidents), as well as reporting immediately to the police.

Other Incidents

In the event of suspicion of other infringements of the policy through careless, irresponsible or deliberate misuse, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in the 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 children and that can, if necessary, be taken off site by police. Use the same computer for the duration of the procedure.
- Ensure that relevant staff have appropriate internet acces 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 be necessary to record and store screen shots of the content on the machine being used for the investigation. These may be printed, signed and attached to the form, except in the case of images of child sexual abuse.
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, the appropriate action required could include:
    - Internal response or discipline procedures
    - Involvement by a national or local organisation
    - Police involvement 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
    - Sending obscene materials to a child
    - Adult material potentially breaching the Obscene Publications Act
    - Criminally racist material
    - Other criminal conduct, activity or materials
- Isolate the computer in questions as best as possible. Any change to its state may hinder a later police investigation.

It is important all the above steps are taken to provide an evidence trail for the school and possibly the police and to 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 and Sanctions

It is important that 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.