Milecastle Primary School
Online Safety Policy

To be reviewed on an annual basis

Introduction

In May 2018, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Milecastle Primary School's programme to comply with the new legislation, it has a suite of Information Governance policies.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework

Scope

All policies in Milecastle Primary School's Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images. Email and Instant Messaging.

Teaching and Learning

Why is Internet use important?

The purpose of Internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for all pupils. Our school has a duty to provide pupils with quality Internet access.

The Designated Safeguarding Lead will be responsible for online safety on a day-to-day basis.

Internet use to enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering by the LA. Our web filtering policy can be found on the online safety section of our website
- Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- We will ensure a comprehensive whole school curriculum response is in place to enable all children to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. All teaching staff have access 'Project Evolve' and are able to use the resources on the website to teach relevant online safety objectives at least once every half term.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- As appropriate, pupils will be taught the importance of cross checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content

Information system security

- School ICT systems security is regularly reviewed and training has been (and will continue to be) delivered to children, staff, governors and parents.
- Virus protection is updated regularly.
- Security strategies are discussed with the LA.

E-mail

Currently none of our pupils use an e-mail account. This may change in the future.

- Pupils may only use approved Purple Mash e-mail accounts, which are solely used within Purple Mash lessons.
- Pupils must immediately tell a teacher if they receive offensive, inappropriate or upsetting e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will monitor e-mails from pupils to external bodies.
- The forwarding of chain letters is not permitted.

Published content and the school Website

- Staff or pupils' personal information will not be published. The contact details on the website should be the school address, e-mail and telephone number.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the School Web site without parental permission, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or published on third-party websites. This is collected when a child joins the school.

- Pupil's work and images will sometimes be published on Seesaw, which is a secure learning platform for each individual class.

- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

- The above information is shared with parents as part of our permission forms which are signed by parents. It is their responsibility to notify us of any changes.

Social networking and personal publishing

The school will educate pupils in the safe use of social networking sites (including all of the below) through half-termly lessons, assemblies and access to Project Evolve.

- The school will block access to social networking sites, unless needed for a specific educational need and permission has been granted by the head teacher.
- Newsgroups are not accessed by pupils at school.
- Pupils are advised never to give out personal details of any kind, which may identify them, their friends or their location.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are given individual usernames and passwords to access their work on Purple Mash.
- Each class has a QR code for access to their pupil folders on Seesaw and they are encouraged not to share this.
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use appropriate nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with the LA to ensure filtering systems are as effective as possible. Our web filtering policy can be found on the online safety section of our website.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing Leader, Head Teacher or Data Manager, who will take the appropriate action. When unsuitable content is accessed by a student, staff are advised to remove the device from the student immediately.
- Children will be given specific devices to use (iPads and PCs) in order for staff to monitor each individual closely
- Every night, smoothwall filter automatically updates accordingly to keep up-to-date with changes to websites and web content.
- All of the above measures will prevent the children from having access to materials and content that is inappropriate. For example: Pupils having access to extremist or terrorist material while using school networks (prevent duty).

Managing video conferencing

- Microsoft Teams will be the chosen videoconferencing system to be used within staff meetings (teachers only) and if relevant for teachers to deliver lessons to children in the event of lockdowns (in the past teachers used Seesaw to deliver lessons in the event of lockdowns or self-isolation).
- IP videoconferencing should use the educational broadband network to ensure quality of service and security.
- Videoconferencing and web cam use will be appropriately supervised for the pupils' age.
- When teachers need to access third-party video conferencing then this must be through an approved website (For example: Zoom, Google Meet or Microsoft Teams).

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering

systems and present a new route to undesirable material and communications.

- Mobile phones will not be used by staff during lessons or formal school time unless permission has been given by the Head Teacher (e.g awaiting a phonecall from the hospital).

- If children bring mobile phones into school then it must be turned off as soon as they enter school grounds and it must be kept in the school office until home time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- When possible, staff will use the school phone to contact parents and carers. When a member of staff needs to use their personal mobile phone to contact a parent, carer or pupil, they must withhold their number and delete the phone number from their recent call list.

- The school will ask all new parents to give consent for access to educational software when they register their child with the school in accordance to GDPR.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource. This is updated on an annual basis and staff are only notified if annual changes have been made.
- The school will maintain a current record of all staff who are granted access to school ICT systems.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials.
- Any person not directly employed by the school will be asked to read a copy of the acceptable use of school ICT resources before being allowed to access the Internet from the school site. Their access will continue to be monitored for the time they are at the school.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective and appropriate.

Handling online safety complaints

- Complaints of Internet misuse within school will be dealt with by the Designated Safeguarding Lead in the first instance. Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the consequences for pupils misusing the Internet.
- Discussions will be held with the LA to establish procedures for handling potentially illegal issues.

Introducing the online safety policy to pupils

- Online Safety rules discussed with the pupils regularly.
- Pupils are informed that network and Internet use will be monitored and appropriately followed up.
- A programme of study in online safety for pupils is in place based on the materials from Purple Mash. This is supplemented by videos and assemblies from Project Evolve.
- The Project Evolve resources use each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World".
- We will ensure a comprehensive whole school curriculum response is in place to enable all children to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. Pupils

also taught about being safe online through various units in their PSHE learning and through additional assemblies and workshops.

- Our Online safety overview is highlight in green on the Computing Curriculum Overview on the website.

- Any online safety issues that are brought forward by a pupil MUST be reported to the Designated Safeguarding Lead.

Staff and the online safety policy

- All staff will be given the school online safety policy and its importance explained.
- Staff understand that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always use a search engine filtered by the LA when accessing the web with pupils. Google is our chosen school search engine.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School online safety Policy in newsletters and on the school web site.
- The school will publish a set of online safety resources for parents/carers on the school website. Parents will be regularly reminded about all of the information on the online safety section of the website.
- The parents and carers are able to sign up to the National Online Safety website as a parent/carer user. This will allow them to have access to courses, videos, parent guides and monthly newsletters.
- Internet issues will be handled sensitively, and parents will be advised accordingly.