Online Safety Policy

E-Safety Responsibility: Miss N Creamer (lead)
Mr J Watling (Deputy lead)
E-Safety Governor: Mr P Bell
Date policy reviewed: September 2023
Signed: (E-Safety lead)
Signed: (E-Safety governor)

Introduction

If any staff member has **any** concerns about a pupil's welfare, they must act on it immediately.

Peer-to-peer abuse is a key factor, especially in cyber-bullying. This is something which must be taken into account in all safeguarding/E-Safety concerns within or outside of school between two or more pupils of Milefield Primary School. Part 5 of KCSiE provides guidance on how you should respond to reports of child-on-child sexual violence and sexual harassment.

The 13-page section explains what schools should do **immediately** after such a report. You must decide whether to:

- Manage the case internally
- Seek early help with a multi-agency approach
- Refer to children's social care
- Report the case to the police

Information sharing is vital to good safeguarding, and fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children. (KCSiE, 2018)

National guidance suggests that it is essential for schools to take a leading role in E-safety.
Becta in its "Safeguarding Children in a Digital World" suggested:
"That schools support parents in understanding the issues and risks associated with children's use of digital technologies."
Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting E-safety messages in home use of ICT too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:
"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

Development / Monitoring / Review of this Policy
This policy has been developed by E-Safety Coordinator – Miss N Creamer
It takes into account discussions/consultations with:
• Headteacher
• Teachers
• Support Staff
• ICT Technical staff
• Governors
• Parents and Carers
Consultation with the whole school community has taken place through the following:
• Staff meetings
• School Parliament
• INSET Day
• Governors' meeting
• Parents' evening
• School website / newsletters / Facebook
The implementation of this E-safety policy will be monitored at regular intervals. The E-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 E-safety or incidents that have taken place.
Should serious E-safety incidents take place, the following external agencies should be informed:
LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office, LADO
The school will monitor the impact of the policy using:
• Logs of reported incidents (CPOMs)
• Internal monitoring data for network activity
• Surveys / questionnaires of:
- pupils
- parents / carers
- staff

Scope of the Policy
This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Roles and Responsibilities
The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school.

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:
• regular monitoring of E-safety incident logs
• regular monitoring of filtering / change control logs
• reporting to relevant Governors meeting

Headteacher and Senior Leaders:
• The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator Miss N Creamer with support from the deputy lead as necessary.
• The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
• The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
• The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
• The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff (see Whistleblowing Policy).

Online Safety Coordinator: Miss N Creamer
• takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety 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 all staff
• liaises with the Local Authority
• liaises with school ICT technical staff
• receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments (CPOMs)
• Discussions held regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
• attends relevant meeting(s)
    - Ensures all staff/governors complete relevant training
    - Invites parents to complete online safety training (Regular invitations each year)
• reports regularly to Headteacher / Senior Leadership Team

ICT Technician: Mr D Wakefield (HCAT)
The ICT Technician is responsible for ensuring:
• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• that the school meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
• that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
• the LA is informed of issues relating to the filtering applied
• the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
• that he / she keeps up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
• that the use of the network / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher / Senior Leader for investigation / action / sanction
• that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:
Teaching and support staff are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current school E-safety policy and practices
• they report any suspected misuse or problem to the E-Safety Co-ordinator / Headteacher / Senior Leader for investigation / action / sanction

- Staff in direct contact with pupils will use CPOMs and log any incidents under the following categories. DSLs will then investigate the situation.

• digital communications with pupils/parents (email / Facebook / Twitter / website) should be on a professional level
• E-safety issues are embedded in all aspects of the curriculum and other school activities
• pupils understand and follow the school E-safety rules established for acceptable use (Class charters)
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (Computing curriculum)
• they monitor ICT activity in lessons, extra-curricular and extended school activities
• they are aware of E-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices (See staff handbook/code of conduct)
• in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Co-ordinator
Mrs K Trickett (Executive head of school), Mr J McClure (Head of school) and Miss L Jones (Pupil welfare leader) are DSL trained so are trained in E-safety issues and are 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

- Peer-to-peer abuse

Pupils:

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
• should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school (Including use of home learning platforms (Seesaw for example))

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' seminars, newsletters, letters, website and information about national / local E-safety campaigns / literature. Parents and carers will be responsible for:

• endorsing (by signature) the Pupil Acceptable Use Policy / Home school agreement (Distributed annually)

Policy Statements

Education – pupils

E-Safety education will be provided in the following ways:

• In accordance with the 2014 National Curriculum requirements, planned E-safety teaching will be provided as part of Computing / PD & RSHE /other curriculum areas (as relevant) and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
• Key E-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
• Pupils should 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 to be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
• Rules for use of school computers / laptops / ipads / internet will be devised annually through discussion with pupils. These will be posted in classrooms
• Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Although, it is recognised many parents and carers have only a limited understanding of E-safety risks and issues, they undoubtedly play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.
With this in mind, the school will therefore seek to provide information and awareness to parents and carers through:

• Letters and newsletters
• Parent workshops
• Reference to relevant online guidance provided by the school website or in paper format by the school office

Education & Training – Staff

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• Formal E-safety training will be made available to staff as part of the termly CPD programme
• All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies
• The E-Safety Co-ordinator will receive regular updates through attendance at ICA meetings and training events / LA courses / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others
• This E-Safety policy and its updates/ current e safety issues will be presented to and discussed by staff in staff meetings
• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required
• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required when using online video conferencing platforms (Teams/Zoom, etc.) All above rules will apply. All participants will be made aware that online conference calls are recorded (when necessary) prior to the commencement of the conference.

Training – Governors

Governors should take part in E-safety training / awareness sessions, with
particular importance for those who are members involved in ICT / E-safety / health and safety / child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

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 named in the above sections will be effective in carrying out their e-safety responsibilities:

• There will be regular reviews and audits of the safety and security of school ICT systems. These will take place every half-term or when an incident occurs.

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school ICT systems.

• All users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames.

• The "administrator" passwords for the school ICT system, used by the ICT Technician must also be available to the Head teacher or other nominated senior leader and kept in a secure place

• Users will be made responsible for the security of their username and password, 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.

• In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be carried out by a process that is agreed by the Headteacher (or other nominated senior leader)

• Any filtering issues should be reported immediately to N.Creamer.

• Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician, Headteacher and Miss N Creamer.

• School ICT technical staff, the Headteacher and Miss N Creamer(pupils only) regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

• An appropriate system is in place for users to report any actual / potential E-safety incident to the Network Manager (or other relevant person). Staff would consult Miss N Creamer and the Headteacher. The issue would be reported on CPOMs and dealt with accordingly.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

• An agreed policy is in place for the provision of temporary access of "guests" (eg students, visitors) onto the school system.

• An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.

• An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.

• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.

• The school infrastructure and individual workstations are protected by up to date virus software.

• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a continuing focus in all areas of the curriculum and staff should reinforce E-safety messages, wherever possible, in the use of Computing across the curriculum.

• We follow the HCAT curriculum in teaching of computing skills. This links granular knowledge to progressive skills and focuses on engaging pupils in real-life situations and purposeful learning. Every new year/term begins with online safety foci and pupils are expected to share their knowledge of these skills. Our curriculum is built in such a way that pupils know more and remember more.

Where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use through bookmarks. Processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, thus encouraging responsible use.

• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician can temporarily remove those sites from the filtered list for the period of study. Any request should also be brought to the attention of the Head teacher and E –safety co-ordinator with clear reasons provided. These will be logged, following each request, then supplied to D. Wakefield (ICT Technician)

• Pupils should 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images
When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
• When using digital/social media – **See acceptable use agreement document.**
Communication technologies
When using communication technologies the school considers the following as good practice:
• The official school email service may be regarded as safe and secure and is monitored.
• Users need to be aware that email communications may be monitored.
• Users must immediately report, to the Headteacher or Miss N Creamer– in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
• Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE, etc.) must be professional in tone and content. Personal email addresses, text messaging or public chat must not be used for these communications; however, school's Facebook and Twitter accounts may be used to communicate as all parties can access and maintain evidence records of communication.
• Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. These strategies will be outlined in each classes' curriculum planning.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
• Pupil - teacher communication is used on Seesaw home learning accounts. Only the allocated teachers and pupils can see these comments and teachers must check comments before they are approved to be posted online. If any communication is deemed inappropriate, staff should notify SLT and not approve this post. They may screenshot and add to CPOMs for evidence. The HT and E Safety lead have access to all home learning accounts for screening purposes.

Data protection
• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act/GDPR 2018

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which determines how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

'Personal data' means information that can identify a living individual.

The regulation applies to all schools, and will apply even after the UK leaves the EU.

The GDPR sets out the **key principles** that all personal data must be processed in line with.

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

New requirements

The GDPR is similar to the Data Protection Act (DPA) 1998 (which schools already complied with), but strengthens many of the DPA's principles. The main changes are:

- Privacy notices must be in clear and plain language and include some extra information – the school's 'legal basis' for processing, the individual's rights in relation to their own data

- Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous

- There are new, special protections for children's data

- The Information Commissioner's Office must be notified within 72 hours of a data breach

- Schools will need to carry out a data protection impact assessment when considering using data in new ways, or implementing new technology to monitor pupils

• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission of the headteacher. Any data which is impractical to ensure is kept in school (eg Reports) will be kept secure, by use of school's online systems only; no personal memory sticks will be used

Acceptable Use Policy

Use of the Internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access.

There are a number of options available that restrict access to the Internet, but it must be understood that no system, other than a ban on using the Internet, can ensure users do not access material that is deemed inappropriate. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying and identity theft which cannot be controlled by filtering systems. For these reasons, treating the use of the Internet as an issue that involves pupils, staff and parents has to be the most sensible approach.

In response to this, the most appropriate course of action is to develop a school policy on use of the Internet together with a home/school agreement.

Milefield Primary School has an Acceptable Use Policy, together with rules for safe internet use. These rules are a joint agreement between staff and pupils as part of our E-Safety curriculum. The policy works in line with our Home School Agreement and is available to parents on request and electronically via our website.

Research using electronic methods is now fundamental to preparing pupils for citizenship and future employment possibilities. The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about E-safety will be planned and that staff will guide pupils in line with Government guidelines.

The school recognises that training the staff in preparation for using the Internet and indeed any mobile technology in a safe manner is vital. The school will use a variety of agencies to train the staff in integrating new technologies into the curriculum. Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and E-Safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference.

The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the E-Safety Co-ordinator. The Co-ordinator will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area. All pupils across the school have access to the Internet and are able to use the technology available. It is anticipated that access to younger pupils will be more directed, with autonomous use being available to older pupils. Where pupils are given freedom to search the Internet for information, they should be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, E safety co-ordinator or the Head. Any incidents will be reported and logged by the E safety co-ordinator using CPOMS.

Pupils will be taught to use e-mail, the Internet and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and pupils at the beginning of each year, rules for Internet access and the use of all technologies within school will be posted in each classroom and around the school. E safety will form an integral part of Computing lessons but will also be covered in regular assemblies and as part of our PSHE programme of study.

The school believes that access to the Internet and mobile devices will enable pupils to explore resources available from libraries, other schools, LAs and commercial content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance.

The final responsibility for use of the Internet and E safety lies with the parents and guardians of our pupils. Therefore, the school asks parents to sign our Home School Agreement and our regular E-safety updates. In doing so, parents are giving their permission for their children to be educated in accordance with school policies. Parents will also be provided with support and guidance in maintaining their children's safety away from school, through regular events in school and through documentation provided on our website. Such information will also be available in hard copies from the school, should this be required. Also, parents will be given access to online safety training and helpful guides from our connection to the National Online Safety portal.

This policy will be reviewed on a regular basis in line with the E-Safety Policy and any technological advances and developments.

Appendix A

Reporting E-safety/cyber-bullying flow chart

Incident occurs / disclosure occurs

Staff member who was first on the scene reports on CPOMS (Online safeguarding reporting tool)

Incident is logged fully and dated

E-Safety (NCreamer)/ Safeguarding leads (Mrs Trickett/Mrs Crosby/Mr McClure/Miss Jones) are made aware of the incident

Safeguarding leads decide whether further action (CP contacted) / contact parents is required

Follow up action recorded on CPOMS

Every half term/ term the incidents are reviewed and further training/support are delivered to staff/pupils/parents where necessary

Incident resolved