Mayfield School
being the best that we can be

Online Safety Policy

Contents

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access always, therefore should be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. The requirement to ensure that children and young people can use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

This Online Safety Policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour for Learning, Safeguarding and Child Protection Policy, Social Media and Data Security.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. This Online Safety Policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use.

Scope

This policy applies to all members of staff, students, volunteers, parents/carers, visitors, the governing body and community users who have access to and are users of the school's IT system, both inside the school grounds and remotely in any capacity.

The Education and Inspections Act 2006 empowers the Co-Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles & Responsibilities

This section outlines the roles and responsibilities for online safety of individuals and groups within the school.

The school's Designated Safeguarding Lead – Mrs Antonia Edghill

The Governing Body's designated Online Safety Governor – Mr Colm Nolan

Governing Body

The Governing Body is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

The role of the Online Safety Governor will include:

- Meetings with the IT staff, IT teaching staff and the school's Designated Safeguarding Lead.
- Regular monitoring of online safety incident logs.
- Reporting to the Governing Body and/or relevant Committee(s).

Co-Headteachers & Senior Leadership Team (SLT)

The Co-Headteachers are responsible for ensuring:

- The safety (including online safety) of all members of the school community, although the day-to-day responsibility for online safety may be delegated to the Designated Safeguarding Lead.
- That adequate training is provided.
- That effective monitoring systems are set up.
- That relevant procedures in the event of an online safety allegation are known and understood.
- That the school's Online Safety Policy and documents are established and reviewed (in conjunction with the Designated Safeguarding Lead).
- That the school's Designated Safeguarding Lead be trained in online safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

Designated Safeguarding Lead

The Designated Safeguarding Lead takes day-to-day responsibility for online safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, the Online Safety Governor and SLT on all issues related to online safety.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Co-ordinating and reviewing online safety education programmes in school.
- Ensuring online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- Overseeing a staff steering team and student digital leaders.

Network Manager

The Network Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets online safety technical requirements.
- The school's password policy is adhered to.
- 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.
- He/She is kept up-to-date with online safety technical information.
- The use of the school's ICT infrastructure (network, remote access, email etc.) is regularly monitored.

Teaching & Support Staff

In addition to elements covered in the Acceptable Use of ICT Systems (Staff) Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the school Acceptable Use of ICT Systems (Staff) Policy (AUP).
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- In lessons where Internet use is pre-planned, students are 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.

Students (to an age appropriate level)

Students are responsible for using the school ICT systems in accordance with the Acceptable Use of ICT Systems (Students) Policy (AUP), which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.

Furthermore,

- Students understand and follow the school's Online Safety Policy and the Acceptable Use of ICT Systems (Students) Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Students should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy also covers their actions out of school, if related to their membership of the school.
- Implement peer education to develop online safety.

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 are. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Acceptable Use of ICT Systems (Students) Policy.
- Accessing the school website in accordance with the relevant Acceptable Use of ICT Systems Policy.
- Attending termly online safety events whereby they can speak to staff about any online safety concerns.
- A partnership approach with home and school, discussing online safety issues with their child.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Receiving and acting on information and guidance suggested regarding online safety from school.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP before being provided with access to school systems.

Education and Training

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Use Policies (AUPs)

All users will be required to sign an appropriate Acceptable Use of ICT Systems Policy Agreement (AUP) before using the ICT system; these are available from the IT Department for staff and students and from main reception for community users.

Parents/carers will be required to read through and sign alongside their child's signature, helping to ensure their child understand the rules.

Staff and regular visitors to the school will be given an AUP that they must read and sign to confirm their understanding of it.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations – staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff/children should open the selected image and go to its website to check for copyright.

Staff Training

- The Designated Safeguarding Lead ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- A planned programme of online safety training is available to all staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy, the Acceptable Use of ICT Systems (Staff) Policy and the Safeguarding and Child Protection Policy.
- The Designated Safeguarding Lead/SLT link will receive regular updates through the Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety, health and safety or child protection.

Communication

Email

Digital communications with students (email, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in the Safeguarding and Child Protection Policy).

The school's email service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems) or Outlook.

Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses.

School email is not to be used for personal use. Staff can use their own email in school (before and after school and during lunchtimes when not working with children) – but not for contact with parents/ students.

Mobile Phones

- School mobile phones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines regarding mobile phone use in school.

Social Networking Sites

- Young people will not be allowed on social networking sites at school; at home it is the parental responsibility.
- Staff should not access social networking sites on school equipment in school or at home.
- Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog.
- Students/Parents/Carers should be aware that the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Students will be taught about online safety on social networking sites as we accept some may use it outside of school.

For more information please refer to the school's Social Media Policy.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of students.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Co-Headteachers.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in their personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

All files downloaded from the Internet, received via email or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.

Websites

In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and processes should be in place for dealing with any unsuitable material that is found in Internet searches.

Staff will preview any recommended sites before use.

"Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research.

All users must observe copyright of materials published on the Internet.

Teachers will carry out a risk assessment regarding which students are allowed access to the Internet with minimal supervision. Minimal supervision means regular checking of the students on the Internet by the member of staff setting the task. All staff are aware that if they pass students working on the Internet they have a role in checking what is being viewed. Students are also aware that all Internet use at school is tracked and logged.

The school only allows the ICT Co-ordinator and SLT to have access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.
- Passwords should be changed at least every 3 months.
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems.

Students

- Should only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten.

Use of Own Equipment

Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Network Manager.

Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

No personally owned applications or software packages should be installed on to school ICT equipment.

Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs.

All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously and selecting Lock) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring and Incident Reporting

It is expected that all members of the school community will be responsible users of the school's ICT systems who understand and follow this policy.

All use of the school's Internet access is logged and the logs are randomly but regularly monitored as a safeguard against inappropriate use.

All online safety incidents must immediately be reported to the Designated Safeguarding Lead in accordance with the school's safeguarding procedures.

Furthermore, anyone who has any suspicion of misuse of the school's ICT systems, deliberate or otherwise, must report it immediately to the Designated Safeguarding Lead in accordance with the safeguarding procedures.

Members of staff should not attempt to investigate any suspicion themselves.

Lessons online

Virtual classrooms or lessons taught online should be treated in the same manner as if students are on site. By using this environment, staff and students agree to the same terms and conditions as laid out in the AUP that all users are required to sign before being granted access to the school's network.