Mayfield Primary School

Policy

E-Safety

Adopted from Cambridgeshire Education ICT Service Model – February 2019

Governor committee to review policy:	Pupil Wellbeing & Learning
Staff member with responsibility for review:	Computing Lead
Date of last review:	June 2020
Date of next review:	June 2023

Online Safety Policy

Contents

Background to this policy:

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age appropriate online safety curriculum for all pupils

Online safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

- The development of our safety policy involved:
    - The Headteacher
    - The Designated Safeguarding Lead
    - The Computing Subject Leader
    - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
    - The governor responsible for Safeguarding

It was presented to the governing body on and ratified on *14.5.20* and will be formally reviewed in *June 2023.*

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and website, and has also been made available to parents.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As Online safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale:

- At Mayfield Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming 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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops, iPads and also desktops in the office and ICT Suite including staff level internet access, server access and access to MIS systems.
- Staff / some staff have access to school systems beyond the school building (e.g. MIS systems, cloud storage of school files). Staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards

Pupils:

- Curriculum laptops / iPads / Chromebooks / desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, Makey Makeys, control equipment, class cameras etc.)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety curriculum:

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- **At KS1:** use technology safely and respectfully, keeping personal information and passwords private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly, keep personal information and passwords private; save and organize files responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Mayfield Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform. ~~(e.g. Starz+, Purple mash, GSuite, O365)~~
- Our programme for online safety education is evidenced in teachers' planning both as discrete, embedded and continuous activities.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.

Continued Professional Development:

- Staff at Mayfield Primary School receive up-to-date information and training on online safety issues in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.
- Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.
- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

School website:

Schools are required to publish certain information online – which in practice means you must have a school website. You are not however required to develop a website policy but sometimes the boundaries of responsibility for setting up, maintaining and ownership of the content are blurred and this can lead to difficulty.

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish as a minimum the statutory information required by the Department for Education.

In conjunction with a range of online services, our school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Head teachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, information displayed on the school website.

The school has established clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Mobile phones and use of data in school:

The Staff Acceptable Use Policy explains the school's approach to mobile phones in school:

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

For pupils:

- Mobile phones being brought into school will be agreed between teachers and parents.
- Children bringing in a device do so at their own risk. The school does not take any responsibility for loss or damage caused to items.
- Devices will be switched off, held securely for the duration of the day by the class teacher, and returned at the end of the day.
- Students will not be allowed to access their devices during the day.
- At the end of the day, children will not use their devices until they have left the school grounds.

Monitoring, and averting online safety incidents:

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network.
- Managed firewalling running Unified threat management (UTM) that provides Restrictions on download of software, apps and file types from known compromised sites.
- Base line and optional enhanced filtering.
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
- Antivirus package provided as part of CPSN Connection.
- Email system for all school staff with direct internal routes to the council for trusted email communications.
- Wireless networks installed by The ICT Service are encrypted to industry best practice standards and the wireless key should be kept securely by the school office.

Staff also monitor pupils' use of technology and, specifically, their activity online.

- Pupils' use of online services (including the World Wide Web) are supervised in school at all times.
- Staff are also able to monitor pupils' activity in the online environment, allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
- Visitors to the school can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case by case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Responding to online safety incidents:

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Mayfield Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

In addition, 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 online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.