Maplewell Hall School

Online Safety Policy

Policy Created	**September 2022**
Governing Body Committee	**FGB**
Date Reviewed by Governing Body	**27.09.23**
Date of Next Review	**Autumn 24**

The Purpose and Scope of this Policy

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation. Technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

At Maplewell Hall School we aim:

- To educate pupils so that they are able to keep themselves safe and legal online;
- Train all staff so that they have the knowledge, skills and understanding to help, educate and support students in online safety;
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors; and
- Establish clear mechanisms to identify, intervene and refer concerns, where appropriate.

Legislation and statutory guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (September 2019), and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation and the Revised Prevent Duty Guidance for England and Wales. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Definitions

Internet enabled Devices

Internet-enabled devices include: Desktop computers; Laptops; Tablets; Smart Phones; Smart TVs; Games' Consoles and any other electronic device capable of accessing the Internet, either via a mobile network provider, Wi-Fi, or Ethernet cable.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Ian Welch.

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

The school's designated safeguarding lead (DSL) is Rob Cooper, Deputy Headteacher (Personal Development.)

The DSL takes overall responsibility for online safety in school. In his absence, the Deputy DSLs will take on all of his responsibilities

Deputy DSL with responsibility for Online Safety

Working with the DSL, the Deputy DSL with responsibility for Online Safety will:

- Ensure that staff understand this policy and that it is being implemented consistently throughout the school;
- Work with the Network Manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensure that any online safety incidents are recorded on MyConcern, appropriately categorised and dealt with in line with this policy;
- Act as case owner for students identified as being at greater risk online;
- Ensure that all safeguarding concerns are seen and dealt with as quickly as possible. All reported safeguarding concerns are 'triaged by the headteacher, the DSL, or a deputy DSL.
- Ensure that any incidents of cyber-bullying are recorded on MyConcern, appropriately categorised and dealt with in line with this policy;
- Ensure staff and governors have access to online safety training through National Online Safety e-learning hub and that staff and governors complete relevant training;
- Liaise with other agencies and/or external services if necessary;
- Provide regular reports on online safety in school to the headteacher and/or governing board.
- Ensure all students are taught how to report online abuse in school and out of school;
- Ensure students have appropriate opportunities to gain nationally recognised qualifications in online safety;
- Ensure all students are taught how to keep themselves safe;
- Monitor and assure the quality of the e-safety curriculum.

The Network Manager

The Network Manager is responsible for line managing the ICT Technician and ensuring that:

- Appropriate filtering and monitoring systems are in place which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- a full security check and monitoring the school's ICT systems is conducted on a monthly basis;

- systems are in place to block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files;
- supporting the planning and delivering of an ICT curriculum that ensures all students understand how they can keep themselves safe online.

ICT/Computing Curriculum Lead

The ICT/Computing Curriculum lead is responsible for line managing the Network manager and:

- the planning and delivering of an ICT curriculum that ensures all students understand how they can keep themselves safe online.
- Ensuring parents and students have access to resources and information to help them stay safe online outside of school.
- Supporting the DSL in the management of safeguarding concerns related to online safety.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1);
- Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the school behaviour policy.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1);
- Complete e-safety training for Parents on the National Online Safety e-learning hub.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Education

Educating pupils about online safety

All staff, governors and volunteers (where appropriate) receive training on e-safety, its impact and ways to support pupils, via the National Online Safety (NOS) e-learning hub.

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** have the opportunity to revisit the key Stage 3 bullet points above. They will also be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The school subscribes to the National Online Safety e-learning hub which gives parents access to a wide range of resources and training. The school will signpost parents to these resources via the school website, letters and the school newsletter.

Where e-safety is a specific concern, school staff may talk directly with parents and carers and signpost them to the e-learning hub.

This policy will also be shared with parents via the school website.

National Online Safety e-learning hub resources will be made available to parents at parents' evenings and other events attended by parents and carers.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with student's tutors.

Concerns or queries about this policy can be raised with the deputy Headteacher (pastoral), Rob Cooper.

The school subscribes to the NOS e-learning hub. This gives parents access to information and training specifically designed for parents. All parents will be signposted towards these resources via the school website, newsletters, letters and phone calls.

In relation to a specific incident of cyber-bullying; online grooming; sexting; and indecent images, the school will follow the processes set out in the Positive Behaviour for learning and Safeguarding and Child Protection policies.

Specific e-safety issues

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

1. **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
2. **contact:** being subjected to harmful online interaction with other users; for example commercial advertising; phishing; and online grooming;
3. **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sexting, sending and receiving explicit images, or online bullying (cyber-bullying);
4. **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams

To help prevent harm caused by online content, contact, conduct or commerce, we will ensure that pupils understand what they are and what to do if they become aware of any of them happening to themselves or others. We will ensure that pupils know how they can report any incidents both in and out of school, and are encouraged to do so, including where they are a witness rather than the victim.

All students will be taught about online dangers associated with content, contact, conduct and commerce, and how to keep themselves safe, as part of their ICT curriculum.

Tutors and other teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Preparation for Adulthood, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining internet-enabled devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found or suspected to be on the device:

- Report immediately to the DSL
- Do not view, copy, print, share, store or save the imagery, or ask a child to share or download.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it. Leave this for the DSL if needed.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).

It is up to the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils using internet enabled devices in school

All pupils may bring internet enabled devices into school.

Students are not permitted to use them during the school day and must hand them in to their tutor at morning register. Students may not use internet enabled devices in lessons or around the main school site without express permission from a member of staff.

Staff may confiscate any devices that are not handed in to their tutor.

Students in key stage 5 may have their internet enabled devices during the school day to support their remote supervision when on school trips and visits.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Positive Behaviour for Learning policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Staff use of personal devices

There are circumstances where the use of personal devices whilst at work is acceptable. These circumstances might include:

- Recording evidence of learning
- Contacting parents/carers
- Accessing online platforms like Go4Schools, MyConcern or Weduc to carry out work-related tasks

Whenever staff use their personal device they should:

- Use a school device if a school device is available, even if their personal device is more convenient
- Ensure all school related documents, images and recordings are stored on the school network or school cloud storage and not on personal devices, drives, or cloud storage

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

All staff and gove4rnors have access to training and resources on the NOS e-learning hub.

Monitoring arrangements

This policy will be reviewed annually by the Deputy Headteacher (Pastoral). At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- The Safeguarding and Child protection policy;
- The Positive Behaviour for Learning policy;
- The Staff Code of Conduct;
- The Preparation for Adulthood framework.