Elmhurst Primary Online Safety Policy 2023/24

Approved by:	**Date:**
Last review on:	
Next review due by:	

Contents

1) Aims

At Elmhurst we are committed to upholding rigorous standards of online safety, treating it with the same level of importance as any other facet of safeguarding. Just as we prioritise the physical and emotional safety of our students, we also prioritise their digital safety. Through comprehensive online safety policies, proactive measures, and continuous education, we ensure that our students can confidently explore the digital world in a secure and responsible manner.

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all members of the school community (including staff, students, volunteers, parents and carers, governors, visitors, contractors etc.) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.

- Facilitating the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children for the risks and opportunities of today's digital world.

- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world.

- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

2) Legislation informing this Policy

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

This policy also 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 greater responsibility 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.

This policy complies with our funding agreement and articles of association.

3) Roles and Responsibilities

It is important that all members of our community work together to develop safe and responsible online behaviours, learning from each other and reporting concerns, and misuse as soon as these become apparent. While this will be a team effort, the following section outlines the online safety roles and responsibilities of individuals and groups within the school.

3.1 Governors

Governors are responsible for the approval of the Online Safety Policy, reviewing its efficacy and holding senior leaders to account for its implementation.

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

Afia Choudhury, Lead governor for Inclusion and safeguarding will take on the role of Online Safety Governor.

All members of the governing body will:

- Ensure they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1).
- support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.2 The Headteacher and Senior Leaders

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

In addition to this:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.

- The headteacher and senior leaders should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher and senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues.
- better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- 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 online safety monitoring role.

3.3 The Designated Safeguarding Lead

The school's safeguarding lead is Jane Nash. Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL takes lead responsibility for online safety in our school, in particular:

- taking day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- having a lead role in establishing and reviewing the school online safety policies/documents.
- take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- promoting an awareness of and commitment to online safety education/ awareness raising across the school.
- liaising with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- providing (or identify sources of) training and advice for staff, governors, parents, carers and learners.

3.5 The Computing Lead

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the PSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

3.4 The IT Technician
The ICT Manager is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- there is clear, safe, and managed control of user access to networks and devices.
- they keep up to date with online safety technical information in order to effectively carry out their role and to inform others when relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring software/systems are implemented and regularly updated as agreed in school policies.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers
All staff, including contractors and agency staff, and volunteers are must ensure that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use policy (Appendix 1).
- They report any suspected misuse or problem on the Safeguarding portal and report to the DSL in line with the school safeguarding procedures.
- All digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems (School Phone, Parentmail, Google Classroom).
- Ensure learners understand the acceptable use policy, have a good understanding of online threats.

- In lessons, where internet use is pre-planned, learners 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.
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

3.6 Parents and Carers

Parents and carers Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with any member of staff or SLT.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website.
- providing them with a copy of the learners' acceptable use agreement.
- seeking their permissions concerning digital images of children.
- Providing training on the measures they can take to promote safe internet use at home.
- Discuss any concerns related to Online Safety during parents evening.
-

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the use of their children's personal devices.
-

3.7 Visitors

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 1).

4) Acceptable Use Policies

All members are subject to the terms set in our Acceptable Use Policies (AUPs). These are a set of guidelines that outline the responsible use of technology resources within the school's digital environment. It applies to all students, staff, and users who access the school's network, devices, software, and online platforms.

Our AUPs aim to ensure safe, respectful, and secure use of technology while protecting the school community from potential risks and misuse. All members are expected to have read

and signed the appropriate AUP that is relevant to their role within the school; this includes learners from each key stage (Appendix 1).

5) Technology and Devices

At Elmhurst, we recognise the importance of cultivating responsible and secure digital practices to protect staff and students. This section outlines our approach to the use of school technology and devices, encompassing a comprehensive set of guidelines and policies designed to create a safe, respectful, and enriching digital environment for all members of our school community.

5.1 Mobile Devices

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Children/staff data should never be downloaded onto a private phone.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.
- **Pupils** may not bring mobile devices into school under any circumstances.

5.2 School Devices outside of school

All staff members will take appropriate steps to ensure school devices remain secure when granted permission to use off site.

This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 1.

Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the IT technician.

5.2 Photography of students

When a pupil joins Elmurst, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken, the member of staff will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Elmhurst, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach students about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We also teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.

5.4 Responding to issues of Misuse

Where a **pupil** misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher and staff authorised

by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

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/staff code of conduct. 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.

5.5 Filtering and Monitoring
Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring.

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At Elmhurst, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the **UK Safer Internet Centre's appropriate filtering submission page here.**

6) The School Website

The school website is a public-facing information portal for the school community with a key reputational value. The school ensures that its online safety policy is followed when publishing content online. This includes using digital images and videos, respecting copyright, and safeguarding the privacy of young individuals. We prioritise minimising risks to our school community. When sharing student work, images, or videos, we ensure full names are not published.

7) Handling Online Safety Concerns

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE and Citizenship). Concerns must be handled in the same way as any other safeguarding concern by reporting on this website.

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

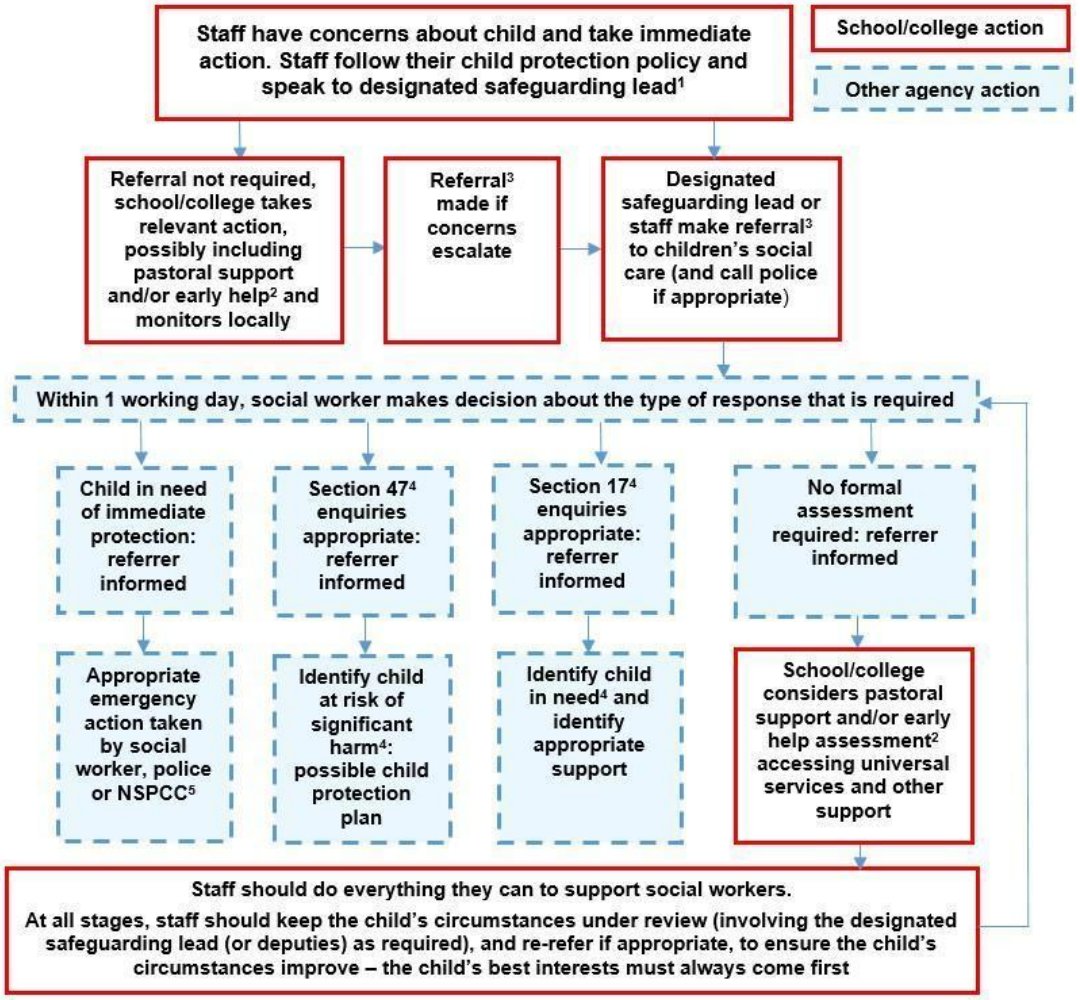
Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

The following flow chart (it cannot be edited) is taken from Keeping Children Safe in Education 2023 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



8) Cyberbullying

8.1 Definition

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

8.2 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 through class work and shared assemblies, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. This is explicitly addressed through our online safety curriculum and the Jigsaw scheme of work in PSHE.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

9) Examining Electronic 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' electronic 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 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 on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material.
- Retain it as evidence (of a criminal offence or a breach of school discipline).
- 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.

10) Teaching and Learning

At Elmhurst, our Online Safety curriculum has been designed to educate our pupils about the threats they may face when navigating online spaces. Through rich discussions and engaging activities, we raise awareness and cultivate responsible and competent users of technology. We emphasise the importance of online communication skills and the ability to critically evaluate digital information. By developing their digital literacy skills, we empower our pupils to be informed decision-makers and active contributors in the digital landscape.

Online safety lessons are taught once every half term and will cover age-appropriate topics based on the following strands:

- Self Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Wellbeing and Lifestyle
- Privacy and Security
- Copyright and Ownership

Although these strands allow teaching and learning to be varied, this is not an exhaustive list. Our curriculum map is dynamic and responsive to contextual safeguarding.

Appendix 1: Staff, Governor and Visitor AUP:
https://docs.google.com/document/d/1WCWNtUYZlA80lKWXcvia1vX4ld-lus9v/edit?usp=drive_link&ouid=115117254894823251116&rtpof=true&sd=true