EARLSMEAD PRIMARY SCHOOL

E-Safety and Use of ICT Policy

SUCCESS *for* ALL

Written by	Nisha Peshawaria
LGB Approved	March 2026
BOT Ratified	March 2026
Date of Next Review	January 2027

MISSION STATEMENT

At Earlsmead Primary School we encourage all members of our school community to strive to be the best they can be and develop new skills that empower them for life-long learning, in order to become confident, valuable, members of society.
We create an inclusive, supportive, safe and challenging environment where all contributions are valued.
Learning is motivating and independence is encouraged, hence all become reflective, self-learning team members with a positive sense of wellbeing and a love of learning.

OUR VISION

Working in partnership with children, parents, staff and governors, as a community we will achieve *Success for All* through:

S*ecuring resilience*
U*nderstanding values and respecting others*
C*ommitting to our learning*
C*ommunity involvement*
E*quality for all*
S*triving to do our very best*
S*etting high expectations*

This policy is linked to the following mandatory school policies: Keeping Children Safe in Education – September 2025 guidance, Safeguarding and Child Protection, Preventing Radicalisation and Extremism, SEND, Code of Conduct, Whistle Blowing, Health and Safety, Behaviour, Anti-Bullying policies and Home School Agreement.

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Introduction

The use of information and communication technology is an integral part of the National Curriculum and is a key skill for everyday life. At Earlsmead Primary School, we recognise that pupils are entitled to quality hardware and software, alongside a structured and progressive approach to the learning of skills needed to enable them to use it effectively. The purpose of this policy is to state how the school intends to make this provision.

Aims

Our main aims are outlined below:

- *To give pupils experience in a wide range of ICT hardware and software.*
- *To enrich and enliven other areas of the curriculum and to support specific learning needs.*
- *To teach children how to use relevant technology safely.*
- *To provide children with the necessary knowledge and skills to make informed choices about using technology beyond the classroom and after their time at school.*
- *To encourage pupils to understand and change the world through computational thinking.*
- *To enable children and teachers to have access to immediate and up-to-date sources of information.*
- *To raise levels of teacher competence and confidence when integrating ICT into their planning, teaching and assessment of children's work (using ICT as an integral part of the processes and management of teaching and learning).*

Purposes

Through our teaching of computing, we will achieve the following:

- *Set out the key principles expected of all members of the school community at Earlsmead Primary School with respect to the use of ICT-based technologies.*
- *Safeguard and protect the children and staff of Earlsmead Primary School.*
- *Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.*
- *Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.*
- *Have clear structures to deal with online abuse such as cyberbullying, which are cross referenced with other school policies.*
- *Encourage responsible, competent, confident and creative users of information and communication technology.*
- *Understand and apply the fundamental principles of computer science, including data representation, systems, algorithms and programming.*
- *Understand the risks involved with using technology and react appropriately*
- *Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.*

To help achieve this, children will have the opportunity to develop skills in:

- The use of hardware.
- Processing and interpreting data.
- Creating media.
- Control and programming activities.
- Searching, organising and presenting data.
- Databases.
- Internet research and other uses.
- Spreadsheet modelling.
- Understanding the role of ICT in society.
- E-safety within each computing topic.

Earlsmead is equipped with interactive whiteboards in each classroom to use as a teaching tool. Other ICT equipment such as tablets are also available to bring ICT into subjects across the curriculum. With this in mind, children will use ICT to support and enhance the learning experience of the wider curriculum. They will develop ICT skills at an appropriate level regardless of race, gender, intellect, emotional or physical difficulties.

What is online safety?

Online safety is defined as educating people about the benefits, risks and responsibilities of using the internet and electronic devices. Online safety is:

- Safeguarding children in the digital world.
- Not about restricting children, but educating them.
- Supporting children and young people to develop safer online behaviours both in and out of school.
- Being educated ourselves to be able to support and help the children.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk as outlined in *Keeping Children Safe in Education, September 2025:*

Content: Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

In particular, children are shown how to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable/unacceptable behaviour online, such as cyberbullying.
- Keep passwords and personal information safe.
- Report when they feel unsafe.

Understand their online presence and how to be in control of their own privacy.

CYBERBULLYING

Cyberbullying is the use of cell phones, instant messaging, email, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone. This is sending or posting harmful or cruel text or images using the internet or other digital communication devices.

It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. This is done by:

- Promoting a culture of confident users will support innovation and safety.
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
  The perpetrator will be asked to remove any material deemed to be inappropriate or offensive. A service provider may be contacted to remove content.
  Internet access may be suspended at school for the user for a period of time. Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.
  Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.
  Pornography – many children will come across some type of pornographic content when searching the internet. Children are taught about what to do if they come across this type of material and who to speak to.

  Contact with violent extremists - Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences. Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.
  Earlsmead Primary School will ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.
  We can help children develop self-awareness, empathy and effective decision-making by regularly asking these questions:

- Am I being kind and showing respect for others and myself?
- How would I feel if someone did the same thing to me, my family or to my best friend?
- What would a trusted adult, someone who is important in my life, think?
- Is this action in violation of any agreements, rules, school policies or laws?
- How would I feel if others found out it was me?
- How does this action reflect on me?

As a school, Earlsmead takes cyberbullying very seriously. We train all our staff to recognise what cyberbullying looks like and how to respond to it, we educate our children about the risks involved and deal with, and monitor, all instances of cyberbullying should it arise.

The Single Point of Contact (Head teacher) and Designated Safeguarding Lead will review all incidents in order to establish whether there are any patterns of extremist groups targeting the school. If there is evidence that a pupil is becoming deeply enmeshed in the extremist narrative, staff should seek advice from Harrow Children's Services on accessing programmes under the Channel project to prevent radicalisation.

ARTIFICIAL INTELLIGENCE (AI)

AI refers to technology that can make computers learn and have human-like intelligence. A machine can be programmed to perform human-like tasks, based on the information it takes from it's surroundings and previous experiences. It uses digital tools and systems that can generate content, analyse information, support learning, or automate tasks. Examples may include writing support tools, image generation tools, or applications that provide suggestions or summaries.

At Earlsmead Primary School, the school recognises that AI tools may have a growing role in education; however, their use must always be safe, appropriate, transparent and age-appropriate.

Acceptable Use

AI tools may be used by staff to support:

- Lesson planning and preparation
- Generating ideas or examples for teaching and learning
- Administrative tasks, such as drafting documents
- Professional reflection and development

Any use of AI should:

- Support, not replace, professional judgement
- Be used responsibly and ethically
- Be aligned with the school's values, safeguarding duties and curriculum aims

Use by Pupils

Pupils are not permitted to independently access or use AI tools unless:

- The activity has been specifically planned and supervised by a member of staff
- The tool and activity are age-appropriate
- Safeguarding and filtering measures are in place

AI tools must not be used by pupils to:

- Complete work on their behalf
- Generate assessed work without teacher guidance
- Access inappropriate, unfiltered or unsupervised content

Data Protection and Safeguarding

Staff must not input personal data into AI tools, including:

- Pupil names
- Personal or sensitive information
- Photographs or recordings of pupils or staff
- Any confidential school information
- School name

All AI use must comply with:

- The School's Data Protection Policy
- The UK GDPR
- The School's Safeguarding and Child Protection Policy

Any concerns relating to the use of AI, including inappropriate outputs or safeguarding issues, must be reported immediately through normal safeguarding procedures.

Professional Responsibility

Staff remain fully responsible for:

- All teaching materials used in lessons
- All information shared with pupils
- Verifying the accuracy, suitability and appropriateness of any AI-generated content.

AI-generated content must always be checked, edited and adapted by staff before being used in school.

Online Safety and Filtering

The school's existing:

- Filtering systems
- Monitoring arrangements
- Acceptable Use Agreements
-

Apply equally to any AI-enabled platforms or tools.

Use of AI must not bypass school systems, safeguards or filtering.

Review and Emerging Technologies

The school acknowledges that AI technology is developing rapidly. This section will be:

- Reviewed regularly
- Updated in line with national guidance, school practice and technological developments

Any new or significant use of AI will be considered in line with the school's safeguarding, e-safety and data protection duties.

Monitoring and Supervision

Adult Supervision: Any AI-based technology, particularly tools such as smart glasses or video systems, should be monitored by teachers or other responsible adults to ensure appropriate and safe use. However, reliance on digital supervision may inadvertently discourage students from developing critical problem-solving skills, as they may come to depend on technology for guidance rather than engaging with content independently.

Classroom Integration: AI tools can be integrated into structured, teacher-guided activities, ensuring that they complement learning rather than distract from it. Nonetheless, when overused, there is a risk that these tools may undermine essential face-to-face interactions and traditional teaching methods.

Everything posted online is public – it can be copied and redistributed – *think before you post.*
The Department for Education has released a document that aims to help parents better understand the issues and offers advice about many aspects. You can download it by clicking below:
https://assets.publishing.service.gov.uk/media/5a81638840f0b6230269709c/Advice_for_parents_on_cyberbullying.pdf

Planning

As a school, we are constantly developing our resources and expertise to deliver the ICT and computing curriculum. Teachers use the KAPOW Computing scheme of work to support the planning process. Units are sequenced to allow clear progression through key stages; this starts with our youngest children in EYFS. Objectives taught within units fully meet the requirements of the National Curriculum and children's termly success is captured in line with our internal assessment processes.

As a school, we are very aware that some children have particular teaching and learning requirements which could present barriers to learning or hinder progress. This could include learners with SEN or academically more-able children. Teachers must take account of these requirements and plan, where necessary, to support individuals or groups of pupils to enable them to participate and succeed.

Assessment

Assessing computing is an important part of teaching and learning and is central to good practice. It should review the way that techniques and skills are applied purposefully by pupils to demonstrate their understanding of concepts. All computing lessons begin with a POP (proof of progress) Quiz. This process recaps over the most important learning points in the unit, encouraging learners to recall this knowledge accurately each week. Over the course of units taught, work produced is recorded in class floor books or saved centrally on the school system in a place that all children and adults have access to. At the end of units taught, a task is carried out which enables learners to showcase the skills they have build upon across the unit. This task both celebrates the learning that has taken place and captures success against national curriculum objectives. Teachers use this range of information available, alongside their general observations in class, to record whether a child is *working towards, expected* or *exceeding* in that unit. Next steps are then put in place to address gaps in learning. This process is carried out termly in key stages one and two.

Teaching and learning

EYFS

Our children's computing journey begins in EYFS. ICT is not just about computers, and early years' environments should feature ICT scenarios based on experiences in the real world, such as role play. In nursery, the children will

begin drawing on touch screen technology and exploring digital books. In reception, they begin to access, understand and interact with a range of technologies and computing programs. Two computers are set up in our reception classes to introduce the children to some of the tools they will use as they progress through the school. Children gain confidence and control through opportunities to 'paint' and there is a strong focus on digital literacy in EYFS. This forms the foundations needed for when they enter KS1.

Key stage one

By the end of KS1, pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digital devices and that programs execute by following precise and unambiguous instructions.
- Create and debug simple programs.
- Use logical reasoning to predict the behaviour of simple programs.
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content.
- Recognise common uses of information technology beyond school.
- Use technology safely and respectfully, keeping personal information private, identifying where to go for help and support when they have concerns about content or contact on the internet, or other online technologies.

Key stage two

By the end of KS2, pupils should be taught to:

- Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems and solving problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs, work with variables and various forms of input and output.
- Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet, how they can provide multiple services, such as the world wide web and the opportunities they offer for communication and collaboration.
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.
- Use technology safely, respectfully and responsibly, recognising acceptable/unacceptable behaviour and identifying a range of ways to report concerns about content and contact.

Learning via the internet

- Earlsmead's internet access is designed specifically for educational use and includes filtering and monitoring appropriate to the age of the pupils. This is provided by LGfL and Smoothwall and is also monitored by Classroom Technology Solutions (CTS).
- Pupils will learn appropriate and safe internet use and their use of internet will be monitored carefully.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Filtering will occur, however if pupils or staff discover unsuitable material online, they will report the matter to the teacher, who in turn informs the ICT leader (Nisha Peshawaria). This is then logged on our E-safety Incident Log with a description of what happened and how the incident was concluded.
- By year 6, pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Pupils will learn how to communicate safely and appropriately over the internet, through online safety objectives embedded into the curriculum offering, E-safety lessons within each unit, internet safety days and PSHE lessons.
- Pupils are not allowed to use personal email or social networking accounts at school.

How will pupils learn to evaluate internet content?

- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its validity.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Advice will be available to staff in the evaluation of web materials and methods of developing pupils critical attitudes.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Head teacher and ICT Co-ordinator.

Communication

A wide range of communication technologies are available and used within the school including email, Class dojo, Parent pay and website. When using communicating technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users are aware that their email communications are monitored. Therefore, staff and pupils should only use the school email system to communicate with others or Governor Hub for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff or governors contact pupils, parents or conduct any school business using a personal email address. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Users must immediately report any communication that makes them feel uncomfortable. If offensive, threatening or bullying in nature the user must not respond to any such communication.
- Any digital communication between staff and parents/pupils and the wider community must be made through official school communication systems and must be professional in tone and content.
- All communications are to be courteous and respectful of professional's experience and status and be compliant with GDPR. Forwarding email chains is to be avoided unless necessary. The best practice is to send a new email to the relevant colleague.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils are taught about the online safety issues relating to communication and strategies to support the pupils if they come into contact with inappropriate communications.
- Pupils may not use personal email in the school.
- Access in school to external personal email may be blocked.
- Staff will not attach unencrypted sensitive data to emails. If sensitive data has to be sent via the internet it will be sent securely.

The school's MLE may be used to store reports to parents during the writing process; the files will **not be transported by portable storage devices unless password encrypted**

Website content

The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully, pupils' full names will not be anywhere on the website and permission from parents or carers will be obtained before any photographs are published on the school website. The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Mobile technologies

Appropriate use of mobile phones will be taught to pupils as part of their online safety programme. Pupils are not permitted to have mobile phones on them personally at school or on trips. If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school if they are traveling home on their own, the following procedure must be followed:

The parent must provide written consent before a mobile phone can be brought into school. Once written consent has been obtained, the child can bring a mobile phone to school. The phone must be switched off and handed in to the class teacher first thing in the morning. The phone can then be collected at home time. The phone is left at the owner's own risk.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Please see our Use of Mobile Phones Policy, available on our school website, for further information on the expectations Earlsmead Primary School places on mobile technologies for staff, children, parents/carers and other visitors to the school.

Use of video recording equipment for teaching and professional development

The school uses school-owned video recording equipment, including a GoPro camera, to support staff professional development, reflective practice and the improvement of teaching and learning. Recordings are used solely to support self-evaluation by the staff member being recorded.

Acceptable Use
- Use is strictly for internal school purposes.
- Participation is voluntary for staff.
- Recordings are not used for performance management, capability or appraisal.
- Recordings are not shared externally or stored on personal devices.
- Staff may only share recordings with close colleagues with consent.

Safeguarding
Recording will only take place in appropriate teaching environments and will never take place in locations where privacy is expected. Any safeguarding concerns arising must be reported in line with the school's Safeguarding Policy.
Storage and Deletion
Recordings are deleted once viewed for reflection and are not retained long term.

Social Networking and Personal Publishing

The school is aware that social networking is used widely for professional and personal purposes. However, parents and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests.
Users can be invited to view personal spaces and leave comments, over which there may be limited control.

Social Networking - Staff:

- Staff are trained, as a part of their online safety training, about the risks of social networking.
- Staff are advised to not refer to matters of school business when engaging with or on social networking sites.
- Staff are advised to act professionally online.
  All school staff should be aware when using social networking sites that anything said, shown or received could be made available to a wider audience than originally intended. They should follow and understand the following principles:
- Employees and individuals otherwise engaged by the school are not permitted to access social networking sites for personal use via school information systems or school equipment at any time.
- They must not accept pupils as 'friends' and must not approach pupils to become their friends on social networking sites. Personal communication of this nature could be considered inappropriate and unprofessional and make that individual vulnerable to allegations.
- Any pupil-initiated communication, or on-line friend requests must be declined and reported to the Headteacher or Designated Safeguarding Lead.
- Staff are advised not to be online friends with ex or recent pupils of the school or other schools.
- They should not share any personal information with any pupil, including personal contact details, personal website addresses or social networking site details.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Staff cannot under any circumstances mention any references to their working lives on any social media.

- *If staff are online 'friends' with any parent/carer linked with the school, they must ensure that they do not disclose any information or otherwise post details which may bring themselves or the school into disrepute. Staff must not engage in any on-line discussion about any child attending the school.*
- *School staff must not disclose, on any social networking site, any information that is confidential to the School, Governing Body, or Local Authority; or post anything that could potentially bring the School, Governing Body or Local Authority into disrepute.*
- *Staff must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the GDPR.*
- *Staff should not post photographs of pupils under any circumstances and should not post photographs of colleagues or others in the school community without their express permission.*
- *Care should be taken to avoid using language which could be deemed as offensive to others.*
- *Staff are strongly advised to take steps to ensure their online personal data is not accessible to anybody they do not wish to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum.*

Social Networking - Pupils:

- *Pupils do not have access to social networking sites on the school system.*
- *Pupils are advised of the age restrictions on social networking sites and the risks of social networking through their E-Safety lessons. Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.*
- *Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.*
- *Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location.*
- *Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals. Pupils should be encouraged to invite known friends only and deny access to others.*
- *Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.*
- *Pupils must immediately tell a teacher if they receive offensive emails.*

Social Networking - Parents:

- *The school recognises that many parents and other family members will have personal social networking accounts which they might use to discuss/share views about school issues with friends and acquaintances. However, it is not the way to raise concerns or complaints as the school will not respond to issues raised on a social networking site. If there are serious allegations being made/concerns being raised, social media or internet sites should not be used to name individuals and make abusive comments.*
- *Parents must not disclose, on any social networking site, any information that is confidential to the School, Governing Body, or Local Authority; or post anything that could potentially bring the School, Governing Body or Local Authority into disrepute.*

The School considers the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- *Naming children or posting any comments about children who attend Earlsmead Primary School*
- *Making allegations about staff or anyone else connected with the school.*
- *Making any posts that could be deemed to be cyber-bullying*
- *Making complaints about the school or staff at the school*
  Making defamatory statements about the school or staff at the school
- *Posting negative or offensive comments about staff or any other individual connected to the school*
- *Posting racist comments*

- Posting comments which threaten violence
- Posting comments or engaging in online discussions with children other than their own

Procedure the school will follow if inappropriate use continues:
The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try to resolve it and to ask that the relevant information is removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this
- Set out the school's concerns to the parent in writing, giving a warning and requesting that the material in question is removed
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene, grossly offensive or is threatening violence
- Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information;
- Take other legal action against the individual following appropriate advice.
- We are committed to resolving difficulties in a constructive manner, through an open and positive dialogue. However, we understand that everyday misunderstandings can cause frustrations and have a negative impact on our relationships. Where issues arise or misconceptions take place, please contact your child's teacher or the Headteacher, who will be available to meet with you and go through the issue and hopefully resolve it. Where issues remain unresolved, please follow the school's complaints procedure. This is available on the school website or a copy can be requested from the school office.
- Parents have opportunities to find out more about social networking sites by attending parent workshops.
- Parents are advised to follow the school social media rules at home with their children.

Regulation of chat, newsgroups and email lists

- Newsgroups and email lists will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

Roles and responsibilities

All staff have a duty of care to the pupils that are in our school. We are all responsible for all aspects of pupil safety, including online safety, whilst in school. We must teach the children online safety skills regularly to help them develop safe online behaviours. Any activity involving internet use needs to be carefully planned and assessed for risk to minimise the possibility of an online safety incident.
If an online safety incident occurs outside of school and affects our children, the school must deal with the incident.

The following section outlines the online safety roles and responsibilities of individuals within our school.

The role of the governing body

The governors will be responsible for:

- The approval of the E Safety and Acceptable Use of ICT Systems policy and for reviewing its effectiveness. This will be carried out by the Governors receiving termly information about any reported online safety incidents.
- Providing a member of the Governing Body to take on the role of monitoring online safety linked in with monitoring safeguarding.

- Reading, understanding and signing the Governor Acceptable Use Policy (AUP).
- Monitoring the implementation of this policy and its effectiveness.
- Monitoring the effectiveness of the ICT curriculum.
- Monitoring the attainment and progress of pupils in ICT.
- Holding the Headteacher and ICT leader to account for pupils' ICT attainment and progress and the delivery of the ICT curriculum.

The role of the Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of all members of the school community, though the day-to-day responsibility for online safety is delegated to the ICT Co-ordinator.

The Headteacher will be responsible for:

- Overseeing the implementation and reviewing of this policy.
- Ensuring the ICT subject leader is fulfilling the responsibilities of the role.
- That they, SLT and the ICT Co-ordinator are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The ICT Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

The role of the ICT subject leader

The ICT subject leader will be responsible for:

- Producing a computing action plan and for the implementation of this Use of ICT Policy across the school.
- Playing a key role in wider school policy development in relation to ICT and teaching and learning.
- Offering help and support to all members of staff in their teaching, planning and assessment of ICT.
- Maintaining resources and advising staff on the use of materials and equipment.
- Monitoring classroom teaching or planning following the school's programme of monitoring.
- Monitoring the children's ICT work, looking at samples of different abilities.
- Leading staff training on new initiatives: this is important to develop curriculum knowledge and for keeping staff up-to-date with any new approaches to learning and assessment.
- Attending appropriate training for continuing professional development.
- Displaying enthusiasm for computing, encouraging staff to share this enthusiasm.
- Keeping parents and governors informed on the implementation of ICT in the school.
- Liaising with all members of staff on how to improve standards.
- Helping staff to use assessment to inform future planning.

The role of the ICT technician (CTS: weekly site visit)

The ICT technician will be responsible for:

- Maintaining and keeping ICT equipment in good working order.
- Dealing with any reports of broken, damaged or faulty equipment.
- Carrying out an audit on all computers once per term, or sooner if identified.
- Adjusting access rights and security privileges in the interest of the school's data, information, network and computers.
- Addressing any concerns regarding e-safety and computer use in a timely fashion, once alerted by the ICT leader.
- Assisting staff with authorised use of ICT facilities, if required.
- Assisting the Headteacher in all matters requiring configuration of security and access rights, and all matters relating to this policy.
- Accessing files and data to solve problems for a user, with their authorisation – if an investigation is required by the Headteacher, authorisation from the user is not required.

The role of the teaching staff:

Teachers will be responsible for:

- Planning and delivering lessons in line with this policy.
- Providing equality of opportunity to all pupils through their teaching approaches and methods.
- Keeping up-to-date assessment records.
- Ensuring pupils' development of knowledge and skills progresses through their learning and understanding of ICT.
- Supporting pupils to catch-up should they not reach the expected standard following a unit's completion.

- Maintaining an enthusiastic approach to ICT.
- Taking part in ICT training and other CPD opportunities, including internet safety.
- Ensuring health and safety practices are carried out.
- Implementing the E-Safety and Use of ICT Policy.
- They report any suspected misuse or problems to the ICT Co-ordinator and Headteacher for investigation, action or sanction.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online safety is embedded into their teaching and that sites are checked for suitability before using them with the pupils.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

The role of the pupils

Pupils will be responsible for:

- Using the school's ICT facilities appropriately.
- Abiding by the school's rules around use of ICT equipment as agreed to in the Use of ICT Policy Agreement.
- Understanding how the use of ICT improves learning.
- Reporting an abuse, cyberbullying, misuse or access to inappropriate materials.
- Understanding the importance of being safe online.
- Adopting good online safety practice when using digital technologies outside of school and understanding that the school E- Safety and Acceptable Use of ICT Systems policy covers their actions out of school, if related to school.

The role of the parents and carers

A partnership approach with parents/carers will be encouraged as parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand the issues relating to online safety through parent workshops, school newsletters and the website and internet issues will be handled sensitively to inform parents without undue alarm. Parents and Carers are encouraged to support the school in promoting good online safety practice and follow the guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parent sections of the website
- Social Networking Sites
- Mobile Phones
- Their children's personal devices which access the internet

Parents and carers will be responsible for:

- Supporting the implementation of ICT and computing where possible by encouraging the use of ICT and computing skills at home, during homework tasks on Class Dojo and through exploring the school's website.
- Promoting online safety expectations and abiding by the school's rules around use of ICT equipment as outlined and agreed to in our Acceptable Use Policy Agreement.

Why is the use of ICT systems so important to our pupils and staff?

- The purpose of ICT and internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- ICT and internet use are a part of the statutory curriculum and a necessary tool for staff and pupils.
- ICT and internet access are an entitlement for pupils who show a responsible and mature approach to its use.
- ICT and the internet are essential elements in 21st century life for education. The school has a duty to provide pupils with quality ICT systems and Internet access as part of their learning experience.

Equal opportunities

All pupils will have equality of access to the use of ICT across the curriculum. The school will guard against gender stereotyping with encouragement given to both girls and boys to engage in ICT related activities. Children of all ages, ability levels and backgrounds will have equal access to ICT resources.

Health and safety

All wires and sockets, where possible, are kept out of the way of pupils. Any other problems are reported to the ICT leader for swift action. Expectations around safe internet use are shared with our pupils (and families) through our Acceptable Use Policy Agreement which is signed to acknowledge agreement of. Class teachers reinforce these expectations regularly in class and every effort will also be made to ensure that children are sitting in the correct position when using the computer. In all areas, consideration is given to health and safety in the location and positioning of equipment.

Implementation of this policy

- The provision of the ICT curriculum will be monitored and assessed by the ICT leader and Headteacher.
- The suitability of all ICT equipment and programs will be assessed (at least termly) and updated, if necessary, by the ICT technician to ensure they are sufficient for effective learning.
- Staff will be provided with high-quality training regarding both curriculum delivery and online safety.
- Any breach of this policy will be reported to the Headteacher.
- Use of the school's internet connection and network will be monitored by the ICT technician.
- The ICT technician has the ability to remotely view or interact with any computers on the school network. This is to help implement this policy and identify and solve any problems.

FILTERING & MONITORING

What is filtering and monitoring?

Filtering systems block access to harmful websites and content.

Monitoring systems:

- Identify when someone searches for or accesses certain types of harmful online content on school devices.
- Identify who is searching for or accessing the harmful content.
- Alert the school about it so we can intervene and respond.
-

We're all responsible for filtering and monitoring.

You can help to make sure the internet is used appropriately by monitoring what your children are accessing on devices at home (e.g. by looking at their screens when using devices and checking search history regularly).

So what systems do we use?

Keeping Children Safe in Education 2023 states that all schools should have appropriate filtering and monitoring systems in place.

- Earlsmead works with CTS, LGfL, LA, DfE, Smoothwall and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.
- The school's broadband access includes filtering appropriate to the age and maturity of pupils. Our online safety lead (Miss Peshawaria) and IT support (CTS) ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.
- Emerging technologies are examined for educational benefit and the Headteacher, in consultation with staff, gives permission for use.
- Access to images is restricted by integrated safe search tools (controlled by Smoothwall) within the search engine.

Record keeping

- All serious incidents involving the use of technology will be logged centrally by the Senior Leadership Team and as part of the pupil or staff record.
- The records created in accordance with this policy may contain personal data. The School has a privacy notice and a Data Protection policy which explains how the School will use personal data about pupils and parents. The privacy notice is published on the School's website. In addition, staff must ensure that they follow the European General Data Protection Regulations (GDPR) when handling personal data created in connection with this policy.

Managing emerging technologies and assessing risks

The digital age is ever changing, and new technologies are consistently emerging. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
Neither the school, nor Harrow LA can accept liability for the material accessed, or any consequences resulting from internet use. Methods to identify, assess and minimise risks will be reviewed regularly and after every breach of this policy.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Mobile phones (or similar mobile devices that can access the internet, record and transmit text, sound, images, etc.) will not be used during lessons or formal school time and children's phones will be kept with the class teacher.
- The recording and sending of abusive or inappropriate text messages, sounds or images (still or moving) is forbidden.
- The school does not permit the inappropriate use or activation of digital, electronic, or other recording technologies to be used on school premises without permission, except those devices that are for clear and direct use by teachers, and pupils with a teacher's permission to facilitate pupils' learning.
- The school will use Smoothwall software to monitor pupil and staff use of the school's ICT systems, warning them of unacceptable use and providing senior staff with irrefutable evidence of misuse which can lead to the withdrawal of access to the school's ICT systems. If serious misuse is detected, the Local Authority or Police may be informed.
- The Chair of Governors will be given the evidence if the Headteacher has been found misusing the ICT systems and relevant actions will be taken.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Breaches of the Policy - Reporting/ Complaints/ Sanctions

All staff and pupils have a responsibility to report online safety incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the pupils, staff or school.

- Responsibility for handling incidents is delegated to the Head teacher. Any complaint about staff misuse must be referred to the Head teacher. In the case of the Head teacher, any complaint must be referred to the Chair of Governors.
- While the Governing Body does not discourage school staff from using social networking sites, staff should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment. The Governing Body reserves the right to take action to remove any content posted by school staff which may adversely affect the reputation of the school or the wider school community or put it at risk of legal action.
- The Headteacher may exercise his/her right to monitor the use of the School's information systems, including internet access, where it is believed unauthorised use may be taking place. If such monitoring detects the unauthorised use of social networking sites, disciplinary action may be taken.
- Pupils and parents will be informed of the complaints procedure via the Rules for responsible Internet and computer network use guidelines.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection Procedures.
- The school has a responsibility to deal with cyber bullying reports whether it is happening inside school or outside school.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the Police must be contacted to establish the legal position and discuss strategies.
- Sanctions for misuse include:
- Interview by Head teacher/SLT/ICT Co-ordinator
- Informing parents or carers
- Removal of Internet or computer access for a period which could ultimately prevent access to files held on the system
- When applicable, police or local authorities may be involved.
- Online safety incidents will be recorded on the E-safety log by the ICT

Co-Ordinator or Head teacher. The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Head teacher.

Reviewing

This policy will be reviewed annually by the ICT and E-safety Leaders.
Any changes made to this policy will be communicated to all members of staff.
All members of staff directly involved with the teaching of ICT are required to familiarise themselves with this policy.