Winchmore School

learning to realise potential

E-Safety Policy

Last Reviewed:	May 2026
Next Review Date:	May 2027
Review Committee:	Educational Performance

CONTENTS

1. Introduction

At Winchmore, ICT:

- Contributes to high quality teaching and learning.
- Enables effective tracking, target setting and the management of intervention strategies.
- Enables focused assessment.
- Supports effective internal and external communication.

However, there are inherent dangers of using this powerful tool in a school environment. It is therefore essential that the school creates a safe ICT learning environment that includes three main elements:

- an effective range of technological tools
- policies and procedure to describe and maintain the acceptable use of the school ICT services and facilities with clear roles and responsibilities
- a comprehensive e-Safety education programme for students, staff and parents.

The e-Safety Policy has been written in accordance with our vision for Winchmore School and is supported by the following school policies: Anti Bullying Policy, Behaviour Policy, Child Protection and Safeguarding Policy, Communication Policy, Complaints Policy, Equality Scheme (2012), Looked After Children Policy, Teaching and Learning Policy, the Curriculum Statement and the Homework Policy.

2. Key Principles

- All students should be able to learn in a safe environment and should not be exposed to inappropriate materials or cyber-bullying.
- All teachers and authorised staff (e.g. Behaviour Team) are responsible for promoting and supporting safe behaviours in their classrooms and following Winchmore's e-Safety protocols and procedures. There is a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials for investigation.
- Students are empowered to report concerns through both digital reporting tools and direct communication with school staff, including Form Tutors, Heads of Year, and the Behaviour Team, as well as trusted adults at home.

3. Aims

- To ensure students can learn in a safe and secure environment, in and out of school.
- To minimise the risk of student exposure to inappropriate material or cyber-bullying.
- To develop secure practice for students when communicating electronically.
- To develop student self-responsibility when communicating electronically.
- To ensure consistent good practice for staff when communicating electronically.
- To ensure all staff are aware of issues relating to e-Safety.
- To provide information, advice and guidance for parents/carers on the use of new technologies.

4. Roles and Responsibilities

Role	Responsibilities
Governing Body	Ensure the e-Safety Policy is implemented, monitored and reviewed
Leadership Team: ● Headteacher ● Assistant Headteachers ● Digital Strategy Lead	Headteacher: ● Ensure, along with the Governing Body, that the e-Safety Policy is implemented, monitored and reviewed (annually). Assistant Headteacher: ● Ensure that all staff are aware of their responsibilities under the policy and are given appropriate training and support so that they can fulfil their responsibilities. Ensure that issues of e-Safety, including cyber-bullying, are addressed within the Computing, RSHE and Citizenship curriculum. ● Leading the e-Safety Management Group.
e-Safety Officer SHI / PCU	● Ensure the School remains 'up to date' with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP) ● Ensure the Headteacher, Senior Leadership Team and Governors are updated as necessary, including being aware of local and national guidance on e-Safety and they are updated at least annually on policy developments
e - Safety Management Group (RMA, PCU, JME, APA)	● Oversee the establishment and maintenance of a safe and secure e - Learning environment at Winchmore School.
Network Manager RMA	● Ensure the School Network is safe and secure for all groups, consistent application of protocols and management and development of software ● Advise Governing Body/Leadership Team on e-Safety issues/technology.
Classroom Teachers + Authorised Staff	● Responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures.

5. The School Network

The security of the School Network is maintained by:

- Ensuring the network is protected through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc.
- Ensuring the network is protected by having Local Authority, Virgin Media, &/or Sophos health checks annually on the network (these may be replaced or updated as appropriate to take account of technical & commercial developments).
- Ensuring the Network Manager is up-to-date with Virgin Media services and policies.
- Ensuring that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately (responsibility of the Network Manager).
- LGFL webscreen.
- Using individual log-ins for students and all other users.
- Never send personal data over the Internet unless it is encrypted or otherwise secured; or sent via secure systems such as egress approved by the local authority.
- Ensuring students only publish within appropriately secure learning environments such as their own closed secure Google classrooms log-in.

6. The Internet

Winchmore recognises that access to the Internet is an invaluable learning tool and vital for effective communication. Safety and security risks are minimised through:

- The supervision of students using the Internet within school at all times, as far as is reasonable, and vigilance in learning resource areas where students have more flexible access.
- The use of LGfL web screening which block sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature and key inappropriate words.
- The use of SENSO (monitoring and management software) which sends concern alerts to the network manager, child protection officer and Digital Strategy Lead.
- Informing users that Internet use is monitored in the Acceptable Usage Agreement, and as part of our student induction process.
- Informing staff and students that they must report any failure of the filtering systems directly to the Network Manager or the classroom teacher.
- Blocking all Chat rooms, AI related platforms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Ensuring that any Internet webcams used outside of the LGfL environment will follow the Consent to video conferencing form.
- Ensuring that any webcams used as part of a video conferencing project are timed, closed and safe. Only using approved sites, such as Google meet/Microsoft Teams.
- Only using approved or verified webcam sites.
- Require students (and their parent/carer) to individually sign an Acceptable Usage Agreement form which is fully explained and used as part of the teaching programme. A copy is kept on file, and this ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Requiring all staff to sign Acceptable Usage Agreement form and keep a copy on their personal file. Ensuring all users know and understand what the 'rules of appropriate use'

are and what sanctions result from misuse through induction and teaching programme.
- Maintaining a record of any cyber-bullying or inappropriate behaviour *(the SIMS Behaviour Log)* and acting to deal with the perpetrators of this behaviour.
- Highlighting information on reporting offensive materials, abuse / bullying etc available for students, staff and parents.
- Immediately referring any material suspected of being illegal to the appropriate authorities – Local Authority and/or the Police.
- Establishing that E Mail and Internet use is not private and the school reserves the right to monitor all E Mails and Internet usage involving the school's IT facilities and/or services
- Allocating an E Mail account through the school (winchmore.enfield.sch.uk) domain – enabling them to access their E Mail from school and at home through Google.
- Discouraging the use of personal E Mail addresses, such as Hotmail - staff are instructed to use the school domain system for all professional purposes.
- Ensuring staff do not communicate with students via their personal Hotmail or through their personal social networking site account (e.g. *Facebook, Instagram* etc.)
- Ensuring staff do not attempt to use their personal social networking site(s) in school. Ensuring staff do not communicate with, or have details of, students on their personal social net-working account or any other electronic device e.g. *Facebook .*
- Ensuring that staff should not have student contact details on their personal mobile phones; except for on the school phones allocated for trips.
- Ensuring that student details are always taken from SIMs, and any new contact details obtained being passed to the school office for updating as appropriate.
- *Blocking in-school access to external personal E Mail accounts for students.*
- Making students aware of the risks and issues associated with communicating through E Mail and to have strategies to deal with inappropriate E Mails, as part of the school's e-Safety and anti-bullying education programme.

.

Note:

Incoming and outgoing E Mails are monitored by Google admin only when they are sent and read via the school network.

7. Digital and Video Images

To prevent the inappropriate use of images of Winchmore students the following is observed:

- Parental consent is obtained when students join the school, and subsequently every year, for the publishing of any photographs, video footage etc of students. This ensures that parents are aware that images of their child may be used to represent the school, and opt out if they do not wish their child's image to be used. Photographs published on the Internet/social media do not have full names attached.
- Digital images/video of students are stored in a restricted Google shared drive on the network and images are deleted within a reasonable time unless an item is specifically kept for a key school publication. Students' names are not used when saving images in the file names in the folder. The school avoids including the full names of students in the credits of any published school produced video materials or anywhere that they can be easily identified from photos or videos.
- The Headteacher/Senior Leadership Team lead takes overall editorial responsibility to ensure that the Website content is accurate and quality of presentation is maintained.
- Uploading of information is restricted to the Network Team and Digital strategy lead, with Heads of Learning and Faculty responsible for overseeing and providing the content in their respective areas. The School Website complies with the school's

guidelines for publications.

- Most material is the school's own work; where other's work is published or linked to, the school credits the sources used and states clearly the author's identity or status.
- The point of contact on the Website is the main school address and telephone number, or occasionally individual Winchmore School domain contact details. Home information or individual private E Mail identities will not be published.
- Staff sign the school's Acceptable Use Policy (including a clause on the use of mobile phones / personal equipment for taking pictures of students).
- Students are only able to publish to their own 'safe' web-portal (Drive) restricted by LGfL in school · Students are taught to be aware of the possible wide range of audiences and how images can be abused in their e-Safety education programme.

8. Cyber Bullying

Winchmore Policy: The use of the Internet, text messages, E Mail, video or audio to bully another student or member of staff will not be tolerated. Bullying can be done verbally, in text or images e.g. graffiti, text messaging, E Mail or postings on websites.

'Cyber bullying' is a form of bullying via communication technology like text messages, E Mails or websites. It takes many forms sending threatening or abusive text messages or E Mails, personally or anonymously, making insulting comments about someone on a website, social networking site (e.g. *Instagram*) or online diary (blog/*X*), making, or sharing, derogatory or embarrassing videos of someone via mobile phone or E Mail.

It should be noted that the use of ICT to bully could be against the law. Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means), may be libelous and contravene the Harassment Act 1997 or the Telecommunications Act 1984.

The nature and consequences of cyber-bullying are addressed in Computing/RSHE lessons at KS3 and 4 and in the Extension Programme at KS5. A range of strategies are recommended to support someone who is the victim of cyber-bullying.

9. Monitoring Arrangements

Winchmore School maintains appropriate monitoring arrangements in relation to all Internet, E Mail and related services and facilities that it provides, and the school will apply these monitoring arrangements to all users. These arrangements may include checking the contents of, and in some instances recording, E Mail messages for the purpose of:

- ascertaining or demonstrating standards which ought to be achieved by those using the facilities preventing or detecting crime
- investigating or detecting unauthorised use of E Mail facilities
- ensuring effective operation of email facilities

The school may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this Policy. These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the school's e-Safety Policy and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Disclaimer

The school may arrange for an appropriate disclaimer to be appended to all E Mail messages that are sent to external addresses from the school, in order to provide necessary legal protection.

10. e-Safety Education

10.1 Students

A comprehensive e-Safety programme is provided for all students. In the Y7 Computing programme students are taught how to make appropriate use of ICT as an invaluable learning tool and how to minimise the risks of using ICT in and out of school. They sign the Acceptable Agreement Form in recognition of this. In Key Stage 3, students learn about key e-Safety topics, including AI threats, online scams, bullying, phishing, the dangers of sharing personal information, and the importance of online etiquette. At Key Stage 4, e-Safety is also integrated into the GCSE Computing, BTEC Level 2 ICT courses, and the Level 3 Computing curriculum.

The impact of cyberbullying and strategies for dealing with it are covered in an assembly and through the RHSE programme. The Safer Internet Day assembly each year covers a new specific topic based on that year's focus and is delivered by the Computing department. During February, students also take part in various e-Safety related activities in Computing lessons and within the RHSE programme.

As part of the Computing and RSHE curriculum, students are explicitly taught how to report e-Safety concerns online and are encouraged to speak to a trusted adult, such as their Form Tutor, Head of Year, or a member of the Behaviour Team.

10.2 Remote Learning

During a period of remote learning due to school closures (i.e. COVID or adverse weather conditions) staff are required to use Google Classroom to communicate with students and to set work.

10.3 Staff

As part of their induction, all new staff can arrange to attend an ICT workshop where e-Safety issues are discussed.

All staff are required to read the e-Safety Policy and sign the Acceptable Usage Policy. e-Safety up-dates are circulated by the ICT Strategy Lead/Network Manager when necessary.

Safeguarding lead and HR provides training and advice for staff and emphasised that technology provides additional means for child protection issues to develop i.e. CPOMS and log in password

10.4 Parents/Carers

Every year an Information Evening is provided for parents that covers e-Safety. Advice and guidance can also be accessed via the School Website (Policies , parent and information tab). A

link is sent to parents to download the National Online safety app, reminders will appear in the School Newsletter.

11. e-Safety Complaints

11.1 Role of School

Our Network manager acts as the first point of contact for any complaint or concern.

Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy and should be recorded on the SIMS Behaviour module.

Complaints related to child protection are dealt with in accordance with the school / Local Authority child protection procedures.

Note:

The school takes all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access or ICT usage.

11.2 Investigation of Complaints

The school will investigate complaints received from both internal and external sources, about any unacceptable use of ICT that involves the school IT facilities.

External complaints will be addressed with reference to our Complaints Policy.

The investigation of facts of a technical nature, e.g. to determine the source of an offending E Mail message, will be undertaken by the Network Manager in conjunction with other departments as appropriate.

Where there is evidence of a criminal offence, consideration will be given to whether the issue will be reported to the police for them to take appropriate action. The school will cooperate with the police and other appropriate external agencies as required in the investigation of alleged offences.

In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then appropriate action will be taken. (As outlined in the KCSIE 2024).

11.3 Action in the Event of a Breach of the Standards of Acceptable Use

In circumstances where there is assessed to be a breach of the standards of acceptable use, the school will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate

member(s) of the Leadership Team and the Network Manager.

Subsequent action will be as described below:

- Indications of non-compliance with the provisions of the e-Safety Policy will be investigated, as appropriate, in accordance with the provisions of the school's Disciplinary Procedures, as applicable to staff and students. Subject to the findings of any such investigation, non-compliance with the provisions of the e-Safety Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct for staff members or exclusion for a student. Furthermore, publication, accessing or storing of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action.
- Complaints of cyber-bullying will be included on the e-Safety Log/SIMs Behaviour Log and dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with the school and Local Authority child protection procedures.
- In the case of child pornography being found, the person or persons suspected should be immediately suspended and the Police called on 101.
- Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): https://www.ceop.police.uk/Safety-Centre/
-

12. Monitoring and Review

Monitoring	• Termly analysis of statistics relating to e-Safety issues taken from SIMs Behaviour e.g. a breakdown of cyber-bullying incidents (E safety Management Group) · • Termly analysis of statistics relating to students' attempts to access inappropriate websites, use of games etc. taken from SENSO and LGFL web filter (Network manager)
Review	• Annual Behaviour Review – section on e-Safety issues • Learning Community Reviews

e-Safety Policy created by e-Safety Management Group May 2027