Information Technology and E-Safety Policy

Last Review: **June 2026**
Update: **November 2026**
Next Review: **By the end of the Autumn Term 2028**

Statement of Intent

The school embraces the opportunities provided by new technology to enhance learning and teaching, and to ensure effective running of the school. We recognise our responsibility to educate students about the potential of IT, so that they can become lifelong learners and take their place in the workforce.

Within the context of our safeguarding responsibilities, we recognise also the need to educate them in the risks associated with IT and to guide them in its safe use. It is the school's duty to ensure that every child in our care is safe, and the same principles apply to the virtual/digital world as in our physical buildings.

Creating a safe IT learning environment includes 3 main elements, each addressed in this policy:

- An effective range of technological tools including AI
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education programme for students, staff and parents.

Purpose of the Policy

This document is drawn up to protect all parties – students, staff and the school – and aims to provide clear advice and guidance on how to minimise risks and deal with any infringements. The original Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors.

Contents

The material is arranged under the following headings:

1. Roles and Responsibilities – how and by whom is e-safety implemented in the school
2. Communication of the Policy – how is understanding of the policy spread
3. Technical and Infrastructure Issues
4. Policy & Procedures
5. Remote Working
6. Email and Social Networking
7. Digital Images
8. Equipment Use
9. Complaints and Sanctions

Appendix 1: Acceptable Use Agreement (Students & parents)

Appendix 2: Acceptable Use Agreement (Staff)

1. Roles and Responsibilities

All members and levels of the JCoSS School community and its stakeholders have a responsibility for e-safety. The Leadership team, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and that compliance with it is monitored.

The Deputy Head (Pastoral) has the role of ensuring that the School is up-to-date with e-safety issues, liaising with the Local Authority and organisations such as The Child Exploitation and Online Protection Service (CEOPS) and Childnet International.

The DSL, with the support of the Network Manager and Senso service provider, ensures that filtering and monitoring is:
- age-appropriate and differentiated by group
- regularly reviewed for effectiveness
- logged with an escalation pathway for serious breaches or safeguarding concerns.

As such, the school complies with the March 2023 Department for Education Filtering and Monitoring Standards, ensuring that our systems are:
- Effective in blocking harmful content (e.g. pornography, self-harm, extremism)
- Monitored in real-time with clear lines of accountability
- Appropriate to students' age and developmental needs.

Governors have an overview of e-safety issues and strategies: one Governor has a responsibility for IT, and governors are made aware as part of Safeguarding briefings of local and national guidance on e-safety. They will meet at least annually with the DSL to ensure effective filtering and monitoring are in place.

All teachers and classroom staff are responsible for promoting e-safety in their classrooms. All staff sign an "Acceptable Use" agreement (see Appendix 1) on joining the school, which sets out their responsibilities and duties for e-safety. They are reminded about e-safety at least yearly.

All students are required to sign an "Acceptable Use" agreement (see Appendix 2) on joining the school. E-safety is embedded into the curriculum and all students are educated about safe and responsible use, how to control and minimise online risks and how to report a problem. The school fosters a 'No Blame' culture and encourages students to report any bullying, abuse or inappropriate materials.

Since we wish to raise the awareness of parents and build a partnership in this important area, all parents are required to counter-sign this agreement, as well as signing a "Child Safety Images" consent form. The School will take active steps to engage with parents over e-safety matters.

1. Communication

An understanding of the safe use of IT is communicated in various ways:

To Students

- An e-safety module is included in the Kvutzah (PSHCE) programmes covering both school and home use. Instruction is given in lessons where students are using the Internet.
- Students are made aware that all use of the school network and Internet traffic is monitored and can be traced to individual users.

To staff

- Staff are made aware that Internet traffic is monitored and can be traced to an individual user. Professional conduct, including adherence to GDPR requirements, is expected at all times.
- Staff who manage filtering systems or monitor IT use will be supervised by members of the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

To parents

- Our partnership with parents extends to issue of IT as to all other areas. This includes, as required, information evenings with demonstrations and suggestions for safe home Internet use, advice on filtering systems and etc
- Pastoral or disciplinary issues arising from a student's use of IT will be handled in the same way as others issues. Parents will be advised accordingly.

2. Technical and Infrastructure Issues

The School:

- maintains filtered broadband connectivity through the LGfL and has additional user-level filtering in-place.
- works with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students; also ensures the Network Manager is up-to-date with LGfL services and policies;
- ensures network 'hygiene' through appropriate anti-virus software, annual health checks and network set-up so staff and students cannot run executable files such as .exe /.vbs etc;
- uses security time-outs on Internet access where relevant, and a robust password system
- uses Senso, a fully managed filtering and monitoring solution, in line with DfE Filtering and Monitoring Standards (March 2023). This service includes real-time keyword alerting, visual capture, device monitoring, and safeguarding escalation. It provides reports directly to designated safeguarding leads for oversight and intervention.
- ensures the Deputy Headteacher, Pastoral (DSL) in collaboration with the Network Manager checks to ensure that the filtering and monitoring methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- logs all internet usage and has network auditing software installed;
- uses individual log-ins for all users, making clear to all users the importance of only using the network under their own user name, and of keeping password details secure
- uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites;
- adheres fully to GDPR legislation regarding personal data;
- ensures students only have access to appropriately secure learning environments;
- utilises "power down" functions for equipment where appropriate;
- controls the connection of devices not owned by the school to the network, and reminds staff and students of the need to keep equipment used at home protected against viruses;
- follows all best practice in regarding to data back-up, including off-site facilities and physical hardware.

3. Policy and procedures:

The school:

- supervises students' use of the Network at all times, as far as is reasonable;
- uses the LGfL filtering system which blocks unsuitable sites.
- Uses appropriate monitoring software to detect mis-use of ICT as well as potential safeguarding concerns relating to use of school ICT.
- requires teachers to preview all sites before use or recommended use, and only uses approved provision for video conferencing, communication with students, webcam etc
- plans curriculum context for Internet use to match students' ability, using age-appropriate material and exercising vigilance when conducting 'raw' image searches
- requires staff and students to report any failure of filtering systems directly to a member of staff. The Network Manager liaises with LGfL where necessary; the school will refer any potentially illegal material to the appropriate authorities, including Police.
-
- has blocked student access to music downloads – except as approved for educational purposes. Requires all staff, students and parents to sign an "Acceptable Use Agreement" and ensures parents give consent for students to use the Internet and other IT facilities as part of this agreement;
- keeps a record of any misuse of the IT facilities, in line with the school behaviour policy; ensures the Designated Senior Staff have appropriate training in e-safety; makes information on reporting offensive materials, abuse/bullying etc available to students, staff and parents;
- has set up the network with separate work areas for students and for staff. As required, staff and students are shown how to save and access work from these areas.

4. Emailing and Social Media

The school:

- does not publish personal e-mail addresses of students or staff on the school website.
- uses anti-virus, email spam and 'phishing' technologies.
- Monitors devices for any problematic behaviour, language or searches – this extends to students' Teams accounts.
- uses secure systems for communication with staff and students, giving added security and allowing audit by the school.
- blocks routine access to social networking sites for staff and students

Student-related

- does not use email addresses that identify students' full names.
- informs students to not use other email accounts on the school system, for enhanced safety.
- prohibits the use of mobile phones to do anything that contravenes this policy
- ensures students are educated in the safe use of email and social networking and in 'netiquette' as part of their learning

Staff-related:

- staff will only use the school's IT network and facilities for professional purposes or for uses deemed reasonable by the Headteacher
- uses only secure email systems for transfers of sensitive information, or password-protected/encrypted documents
- requires staff to observe professional standards when using electronic communication

- instructs staff to exercise caution in their use of social networking sites, and not to become 'friends' with any students currently at the school

5. Use of AI

The School:

- prohibits the use of external or public AI systems for processing any personal, sensitive or confidential school data.
- educates students about the risks and benefits of AI, including the potential for deepfakes, misinformation and privacy violations, and encourages critical evaluation of AI-generated content.

Student-related:

- prohibits the use of AI tools except with express permission from a member of staff
- requires students to declare any use of AI in producing their school work

Staff-related:

Until the school procures institutional AI subscriptions with appropriate Data Processing Agreements, staff may use AI tools for professional purposes under the following conditions:

- AI tools may only be used for general professional tasks such as lesson planning, resource creation, policy drafting, and professional development that do not involve inputting any student, staff or school-specific personal or confidential data.
- Any use of AI tools involving even anonymised student or staff information requires prior approval from the Headteacher and must be documented with a risk assessment.
- Staff must comply with all data protection requirements and must not input any information from school systems (Arbor, CPOMS, etc.) or any identifiable personal data into external AI tools.
- Senior leaders using AI tools for strategic planning or policy development must follow the school's SLT AI Guidance document.
- All AI-generated content used in teaching or school communications must be reviewed for accuracy, appropriateness and bias before use.

The school is actively working toward procuring appropriate institutional AI tools with proper safeguarding and data protection controls.

6. Remote Working

In order to manage school closure or absence, staff may at times need to use remote working software such as Microsoft Teams whilst in school or when at home. This applies to both teaching, learning support and administrative staff. Fuller details of expectations relating to teaching and learning remotely are set out in the Remote & Blended Learning Policy.

General principles of remote working, which apply to all staff, are:

- Working hours remain the same, as do normal expectations about attendance and timekeeping for lessons, appointments, meetings etc. Due allowance will be made for the greater unpredictability of home working
- The presumption remains that colleagues should be on site during their contracted hours unless directed otherwise, even if other staff or students are at home. However, the possibility of remote working does not override normal arrangements for illness or other absence. Those who are unwell are not required to work.

- Only the school systems should be used for school communication, meetings, lessons or other contact with students, parents or other agencies
- The school's Microsoft Teams subscription is restricted to use within JCoSS (staff and students). Staff may join Teams meetings with third parties but only if the meeting is set up by the third party.
- The school has multiple Zoom subscriptions which are managed by the Office Manager to avoid clashes
- Due care should be exercised when working on screen to ensure that the background is appropriate, that professional dress is worn and that meetings and lessons can proceed without distraction as far as possible
- All lessons must be recorded; other meetings (e.g. staff or team briefings) may be recorded if desired, but this must be announced on each occasion

7. Digital Images

- the Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- uploading of information to the school website is restricted to named staff.
- the school web site complies with the school's guidelines for publications: most material is the school's own work; others' work is credited appropriately;
- the point of contact on the web site is the school address and telephone number, and no personal or individual identities are published;
- parental permission for use of digital photographs or video involving students is gathered as part of the school agreement form when students join the school.
- Digital images/video of students are stored on the network only; we do not use students' names when saving images or publishing to the school website
- The creation, distribution or use of AI-generated deepfakes or manipulated media depicting students or staff is strictly prohibited and will be treated as a serious safeguarding concern. Any such content must be reported immediately to the DSL
- the Acceptable Use Policy for Staff includes a clause on appropriate use of school equipment for taking pictures of students;

- Students are taught about matching content to audience and about how images can be abused, as part of PSHCE programmes
- Misuse of video or still images from online learning will result in the removal of access to remote learning in one or more subjects either temporarily or permanently
- Misuse of other video or still images of staff or students in school will be dealt with using the Behaviour Management Policy

8. Equipment Use

The School:

- maintains equipment to ensure Health and Safety is followed;
- manages access to student/staff data (MIS system) so that staff users can only access modules related to their role;
- ensures that remote access to the school's network resources is only through approved systems, and does not allow outside agencies to access the network remotely except where there is a clear professional need
- follows LA advice on network security and ensures firewalls and routers are configured to prevent unauthorised use;
- reviews the school IT systems periodically with regard to security;

- does not permit students to use mobile phones other than for specified educational purposes where the Acceptable Use Agreement is followed in full;
- advises staff against use of their personal phones in the presence of students other than in exceptional circumstances, for the protection of all.

9. Complaints and Sanctions

The school takes all reasonable precautions to ensure e-safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements in use and possible sanctions which could be applied as part of the overall Behaviour Policy. Responses might include:

- interview/counselling by staff up to and including the Headteacher;
- informing parents;
- removal of Internet, AI tools or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework;
- removal of access to remote learning in one or more subjects
- mandatory re-education sessions on appropriate AI use and digital ethics
- in cases involving deepfakes or other serious safeguarding concerns, immediate escalation to the DSL
- in cases of serious data protection breaches, immediate escalation to the Data Protection Officer
- referral to LA/Police.

The School Office is the first point of contact for general e-safety complaints. Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to safeguarding are dealt with in accordance with safeguarding procedures.

Staff misuse or abuse of IT facilities is dealt with as part of the normal disciplinary procedures.

Appendix 1: Acceptable Use for Staff

JCoSS IT Network, Internet and Equipment: Acceptable Use Agreement for Staff

Information technology is an expected part of daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this agreement and adhere at all times to its contents.

General IT Use:

- I will only use the school's IT network and facilities for professional purposes or for uses deemed reasonable by the Headteacher.
- I will use only the school's approved systems for official school business.
- I will ensure that all communication with students and staff are compatible with my professional role. In particular, I will not communicate with JCoSS students on social media.
- I will ensure that all my online activity, professional and private, in school and outside school, will not bring my professional role or the school into disrepute.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that personal data on staff or pupils is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Use of AI Tools:

- I will only use school-approved AI tools and must not upload or input any student, staff or other personal/sensitive information into any external or public AI system (including images, audio, text, class data or safeguarding information).
- I understand that all AI use must comply with GDPR and school data protection policies, ensuring no confidential or identifiable information is shared, stored or processed by AI tools unless explicitly authorised by appropriate staff (e.g. SLT, governors, Data Manager, IT).
- I will review all AI-generated content for accuracy, bias and appropriateness, ensuring AI does not replace professional judgement in teaching, assessment, pastoral care or safeguarding, and will report any concerns regarding misuse of AI tools.

Mobile Phones and Digital Images:

- I will only permit student use of mobile phones for educational activities, and will ensure that the Acceptable Use Agreement for students is followed at all times.
- In line with safeguarding guidance, I will not use my mobile phone in the presence of students other than in exceptional circumstances
- I understand that images of students will only be stored and used for professional purposes in line with school policy and with written consent of parents. I will not take images of students using my mobile phone. If using a digital camera, I will ensure that images are stored only on a school-issued memory card and not taken home. Any such images will be transferred to the school server and deleted from the memory card as soon as practicable. Images will not be distributed outside the school network without parental permission.

Monitoring and Remote Working:

- I understand that all my use of the school network or devices, on or off the premises, can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I understand that, if using personal devices (e.g. BYOD), this Acceptable Use Policy applies in full if connecting to the school network or using school systems. Monitoring software may apply to these devices while connected.
- I will respect copyright and intellectual property rights.
- When working remotely, I will follow the school's guidance and maintain normal professional standards of appearance (including backgrounds), behaviour and data security

General Responsibilities:

- I will support and promote the school's e-safety and Data Security policies and help students to be safe and responsible in their use of IT.

I agree to abide by all aspects of the Acceptable Use Policy for the JCoSS Network.

Full Name (printed) .....

Job title ..... Date of Appointment.....

Signature ..... Date.....

Appendix 2: Acceptable Use for Students

JCoSS Network, Internet and Equipment: Acceptable Use Agreement for Students

Information Technology opens up a world of opportunity. With this opportunity also comes danger – some people do not use these technologies to make our world a better place. This agreement helps to ensure that all members of our community use IT in a safe and responsible manner.

General IT Use:

- I will only use the School's IT systems for purposes permitted by the School.
- I will treat all IT hardware with care and respect, and notify any damage to a member of staff. I will not download or install software onto school hardware or network.
- I will only log on to the school network with my own user name and password. I will follow the school's IT security system and not reveal passwords to anyone; to keep my data secure, I will change my password when required. I will not attempt to bypass the internet filtering system.
- I will make sure that all communication with students or members of staff is responsible, considerate and sensible. I will be responsible for my behaviour when using the Internet. This includes the resources I access and the language I use.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress, nor bring any of us into disrepute.

Use of AI Tools:

- I will only use AI tools when my teacher gives me permission to do so.
- I will protect my own privacy and that of others by not inputting or sharing personal information, names, photographs or any content involving other students or staff into any AI system.
- When I submit work for marking, I will acknowledge if I have used AI tools to help create any part of it, and will follow my teacher's guidance on how AI can be appropriately used. I understand that exam boards have strict rules about AI use in coursework and Non-Exam Assessments (NEAs), and that inappropriate use of AI in assessed work may constitute malpractice.
- I will not create, edit or share AI-generated images, videos, voice clips or deepfakes (fake videos or images that look real) of anyone. I understand that creating deepfakes of real people without their consent is illegal and can cause serious harm.
- I will use critical thinking to check whether online content might be artificially created or misleading, and will report any suspicious or harmful AI-generated content to a trusted adult.

Remote Learning and Online Behaviour:

- When using remote learning software, I will continue to abide by all normal school behaviour rules and follow the instructions of teachers regarding camera use, asking for help where necessary
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- I will take extreme care in providing any personal information online. I will not arrange to meet anyone in person without the knowledge and agreement of my parents.

Digital Images and Privacy:

- I understand that images of students and staff will only be taken, stored and used for school purposes in line with school policy.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not take, share, or post images, audio, or video recordings of staff or students without permission.

Mobile Phones and Monitoring:

- I will not use a mobile phone in school other than with the express permission of a member of staff for specified educational purposes.
- I understand that all my use of the Internet and other related technologies can be monitored and logged

and can be made available to my teachers and that this applies whether I am using school devices (both on and off site) or my own device via the school's Wi-Fi network.

- I will not attempt to bypass or disable the school's internet filtering or monitoring tools in any way.

Understanding Consequences

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents may be contacted. In serious cases, such as those involving illegal content or deepfakes, the police may be involved.

Student's Name ..... Form ……..

Student's Signature ……..... Date.....

I consent to my child being given access to the school's IT Network. I note the contents of this agreement and will support the school in its implementation. I am mindful of the need to ensure e-safety at home.

Parent's Signature..... Date.....