JCoSS
JEWISH COMMUNITY SECONDARY SCHOOL

Information and Communications Technology and E-Safety Policy

Adopted: July 2014
Next Review: July 17

Statement of Intent

The school embraces the opportunities provided by new technologies to enhance learning and teaching and to ensure effective running of the school as an organisation and a community. In the context of the *Every Child Matters* agenda, the School takes seriously its responsibility to educate students about the potential of ICT, so that they can become lifelong learners and take their place in the workforce.

We take equally seriously our duty to educate them in the risks associated with ICT and guide them as to its safe use. It is the duty of the school to ensure that every child in our care is safe, and the same principles apply to the 'virtual' or digital world as apply to the school's physical buildings.

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

- An effective range of technological tools
- 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 – the students, the 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

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 school's **e-Safety Co-ordinator** has the role of ensuring that the School is up-to-date with e-Safety issues, liaising with the Local Authority e-Safety Officer and organisations such as The Child Exploitation and Online Protection (CEOP) and Childnet International.

Governors have an overview of e-Safety issues and strategies: one Governor has a responsibility for ICT, and all governors are made aware of local and national guidance on e-Safety and are updated regularly on policy developments.

All teachers 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 matters 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.

2. Communication

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

To Students

- An e-safety module will be included in the PSHCE programmes covering both school and home use. Instruction will also be 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 the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management 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

- We seek to take a partnership approach with parents. This might include information evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

- Pastoral or disciplinary issues arising from a student's use of ICT will be handled sensitively but firmly, and parents will be advised accordingly.

3. Technical and Infrastructure Issues

The School:

- Maintains filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network; 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 health through appropriate anti-virus software, annual health checks and network set-up so staff and students cannot download executable files such as .exe /.vbs etc;
- Uses security time-outs on Internet access where relevant
- Ensures the Network Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Always logs internet usage;
- Has network auditing software installed;
- Uses individual log-ins for all users; and makes clear to all users the importance of only using the network under their own user name
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites;
- Never sends personal data over the Internet or allows it off-site unless it is encrypted or otherwise secured;
- Ensures students only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform via LGFL Security Policies.
- Utilises "power down" functions for equipment where appropriate.
- Restricts the connection of devices to the network not owned by the school; and reminds staff of the need to keep equipment used at home protected against viruses

4. Policy and procedures:

The school:

- Supervises students' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older students have more flexible access;
- Uses the pan-London LGfL filtering system which blocks unsuitable sites.
- Ensures that all sites are previewed before use, or are taken from managed 'safe' environments; and only uses approved provision for students' online creative areas, video conferencing activity, webcam etc
- Plans the curriculum context for Internet use to match students' ability, using age-appropriate search engines and exercising particular vigilance when conducting 'raw' image search with students
- Informs staff and students that that they must report any failure of the filtering systems directly to a member of staff. The Network Manager reports to LA/LGfL where necessary; we immediately refer any material we suspect is illegal or disturbing to the appropriate authorities, including Police and LA.
- Has blocked student access to music download or shopping sites – except those approved for educational purposes.
- Requires all staff, students and parents to sign an "Acceptable Use Agreement" which is fully explained and used as part of the induction/teaching programme; we also ensure parents provide consent for students to use the Internet, as well as other ICT technologies, as part of this agreement; Staff compliance with this requirement is the responsibility of the office staff; student/parent compliance is the responsibility of the data manager.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or misuse of the ICT facilities, in line with the school behaviour management system; ensures the Child Protection Officer has appropriate training in e-safety issues; makes information on reporting offensive materials, abuse/bullying etc available for students, staff and parents;
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.

5. Emailing and Social Networking Sites

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.
- Uses LGFL Mail for communication with staff and other students, giving added security and allowing audit by the school.
- Blocks access to social networking sites except for specific educational purposes (e.g. Internet Literacy lessons)

Student-related

- Does not use email that identifies the students' name or school.
- Prevents students from using 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 e-mail and social networking and in 'netiquette' as part of their learning

Staff-related:

- Staff will only use the school's ICT network and facilities for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- Uses only 'closed' LA secure email system for transfers of sensitive information, or password-protected/encrypted documents
- Requires staff to exercise care when sending e-mails to parents or external organizations.
- Instructs staff to exercise caution in their use of social networking sites, and not to become 'friends' with any students currently at the school

6. Digital Images

At JCoSS:

- 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; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities are not published;
- We gain parental permission for use of digital photographs or video involving students 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 in the file names or in the <ALT> tags when publishing to the school website;
- The Acceptable Use Policy for Staff includes a clause on appropriate use of school equipment for taking pictures of students;
- Students are only able to publish to their own 'safe' web-portal on the LGfL in school;
- Students are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work; they are also are taught about how images can be abused in their e-Safety education programme

7. Equipment Use

The School:

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, Personnel system etc
- Maintains equipment to ensure Health and Safety is followed;

- Manages access to the Management Information System so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems periodically with regard to security.

8. Complaints and Sanctions

The school will take 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.

Staff and students are given information about infringements in use and possible sanctions attached to them which are applied as part of the overall Behaviour Management System. Sanctions available include:

- interview/counselling by tutor/YLC/e-Safety Coordinator/Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework;
- referral to LA/Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

Staff misuse or abuse of the ICT facilities will be dealt with as part of the normal disciplinary procedures.

Appendix 1: Acceptable Use for Staff

JCOSS network, internet and e-mail: Acceptable Use Agreement for Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our 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 ICT. All staff are expected to sign this agreement and adhere at all times to its contents.

- I will only use the school's ICT network and facilities for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will use only the approved, secure e-mail system for any school business.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role. In particular, I will not communicate with JCoSS students on social networking sites
- 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 ICT 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.
- I understand that images of pupils and staff will only be taken with school equipment, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

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 e-mail: Acceptable Use Agreement for Students

Internet and email open us to 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 ICT in a safe and responsible manner.

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will treat all ICT hardware with care and respect and notify any damage to a member of staff. I will not download or install software on school technologies.
- I will only log on to the school network/MLE with my own user name and password. I will follow the school's ICT security system and not reveal my passwords to anyone; to keep my data secure, I will change my password when required.
- I will make sure that all ICT communication with pupils, teachers or others 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, pupils or others distress, nor will it bring any of us into disrepute.
- 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 not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by school staff with the knowledge and agreement of my parents/carers.
- I understand that images of pupils 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 attempt to bypass the internet filtering system. I will not use a mobile phone in school to do anything forbidden by this agreement.
- 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.
- 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 parent/carer may be contacted.

Student's Name ..... Form .....

Student's Signature ..... Date.....

I consent to my son/daughter being given access to the school's ICT Network, Internet and email facilities. 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.....