Redbridge High School e-Safety Policy

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. This Policy 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 how to deal with any infringements.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The responsibility for e-Safety has been designated to a member of the senior management team. Our school e-Safety Co-ordinator is Peter Chadwick a member of the SLT.

Our e-Safety Co-ordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority and through organisations such as The Child Exploitation and Online Protection (CEOP)[6]. The school's e-Safety Co-ordinator ensures the Head, senior management and Governors are updated as necessary. Governors need to have an understanding of e-Safety issues and strategies at this school.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communications services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile 'phones and digital cameras
- Publication of student information/photographs and use of website
- eBullying/Cyberbullying procedures
- Their role in providing e-Safety education for students.
- Data Protection
- Portable storage devices

Redbridge High School e-Safety Policy

How will complaints regarding E-Safety be handled?

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.

Staff and students are given information about uses that are considered infringements.

Our e-Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher and complaints of cyberbullying are dealt with in accordance with our behaviour policy.

Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

General Guidelines for all school internet users (including visitors and guests)

- Virus protection is installed on all computers used for internet access
- Any unsuitable material inadvertently discovered on the internet by a school user must be reported to the e-Safety Co-ordinator/ICT Officer straightaway, who will take appropriate action to block future access to that site
- Copyright of materials and intellectual property rights must be respected
- Internet at Redbridge is for school-related work

School Websites

Official School website:

- Is the official site with main contact details, prospectus information and other potential information which may pertain to the general public
- This website is the editorial responsibility of the headteacher who ensures that the content is accurate and quality of presentation is maintained
- Any student images posted on the website must have had parental/guardian consent.

Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource

- The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave.
- Throughout the school students' access to the Internet will be via the schools network.
- Parents will be asked to sign and return the ??? *Form???*

MANAGING E-MAIL SAFELY

Students

- Students are introduced to, and use e-mail as part of the ICT scheme of work and given guidance on safe and acceptable use and reporting procedures
- Students are advised that they must keep their logins and passwords safe

Staff

- Staff can use the Redbridge/school domain e-mail accounts or web-based e-mails for professional purposes or for legitimate personal uses deemed 'reasonable' by the Head and Governing Body
- Staff are responsible for the content of all outgoing and incoming e-mail and will ensure acceptability of the content; and will handle any inappropriate material they receive in such a way as to help protect the school's ICT resources and shield others form harmful or offensive material

MANAGING DIGITAL IMAGES AND VIDEO SAFELY

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
- If any parent or guardian does not give or withdraw consent this information will be made known to staff teams.

USING THE SCHOOL NETWORK EQUIPMENT AND DATA SAFELY

This school:

- Ensures staff read and sign that they have understood the school's Acceptable Use Agreement / Code of conduct policy. Following this, they are set-up with internet and email access and can be given an individual network login username and password
- Provides students with a class and/or individual network login usernames and if relevant email addresses and passwords
- Makes it clear that staff and students must keep their individual login username and password private and must not leave them where others can find them
- Makes clear that students should never be allowed to logon using a teacher or logins

- Confidential data is kept on the shared drive and is only accessible to staff members.
- Allows teachers to have their own My Documents and is responsible for maintaining their own files
- Has set up the network with a shared storage areas for students and separate ones for staff. Staff and students are shown how to save work and access work from these areas
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities.
- Staff are responsible for data contained on portable storage devices.

Staff Acceptable Use Agreement / Code of conduct

All staff are required to sign an Acceptable User Agreement and Code of Conduct agreement.