The Royal Liberty School

"Where boys are ambitious, where boys succeed

E-SAFETY

E-SAFETY helping your son stay safe

SCHOOL	
Reviewed by:	Deputy Headteacher
Review Date:	May 2018
Next Review:	May 2019

E-Safety encompasses all electronic communications, including Internet technologies, mobile devices as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience.

The school's e-Safety Policy has been rewritten to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole and incorporate the use of emerging technologies. It will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.

Both this policy and the Acceptable Use Agreement are inclusive of:

- both fixed and mobile internet
- technologies provided by the school (such as PCs, laptops, Chromebooks, tablets, whiteboards, digital video and audio equipment, etc);
- technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, gaming devices and tablets, etc).

Introduction

IT in the 21st century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking e.g. Twitter, Facebook, Instagram and Snapchat
- Blogs and Wikis
- Podcasting
- Video Broadcasting and sharing
- Downloading
- Gaming

- Mobile/ Smart phones with text, video and web functionality
- Other mobile devices with web functionality such as tablets and gaming machines
- On-demand TV and video, movies and radio/smart TVs
- Wearable technology e.g. Smart Watches and Fitbits

While exciting and beneficial both in and out of the context of education, much ICT is not consistently policed, particularly web-based resources. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements (13 years in most cases).

At the Royal Liberty School, we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Royal Liberty School holds personal data on learners, staff and others to help us conduct our day to day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in damaging consequences for the individuals and the school as this would break the Data Protection Act (1998)/GDPR. The Trust holds the data protection policy.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. All staff have completed GDPR training and aware of the requirements and legislation.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety coordinator in our school is Mr Henry who has been designated this role as a member of the Senior Leadership Team. It is the role of the eSafety coordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior Leadership Team and Governors are updated by the Head/eSafety coordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's Acceptable Use Agreements for staff, Governors, visitors and students, is used to protect the interests and safety of the whole school community.

E-Safety Skills Development for Staff

- Our staff receive information on e-Safety issues in the form of training opportunities, inhouse communications and via our website.
- New staff receive information on the school's e-safety policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community
- Our staff, Governors and visitors (if appropriate) all agree to an Acceptable Use Policy. The AUP appears on every PC upon login and everyone has to agree before login in.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas as appropriate.

Managing the School E-Safety Messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- E-safety is part of our annual assembly programme for all year groups
- E-safety posters will be prominently displayed around the school's ICT facilities and other visible areas of the school
- E-safety and the policies and guidance are on the school's website.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school has a framework for teaching e-safety as part of the Computing scheme of work and this is revisited annually.
- The school provides opportunities within a range of curriculum areas to teach about e-safety.

- Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- The school responds to recent events both locally and nationally to deliver guidance on the safe practice of the Internet through ad hoc communication with staff, students and parents. E.g. Grooming, sexting and cyberbullying.
- Students are aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teaching.

Monitoring

Authorised IT staff may inspect any IT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact Mr Henry or another member of SLT. Any IT authorised staff member will be happy to comply with this request.

IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving the school's employees or contractors, without consent, to the extent permitted by law. This may be: to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998/GDPR; or to prevent or detect crime. The Trust hold the data protection policy.

IT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business related issues retained on that account.

The Royal Liberty School uses an educational filtering monitoring service via a company called eSafe. The eSafe Service is an intelligence-led early warning system that detects inappropriate IT activity. It uses forensic techniques to monitor imagery, language, Internet activity and off-line use and informs as appropriate those charged with child safety of evident abuse.

The eSafe Service is a completely outsourced, managed service with all server hosting, incident monitoring, incident reporting and escalation, parameter setting and configuration and software systems updates and maintenance performed by eSafe staff.

e-Safe provides full 24x7 monitoring of school-owned devices by staff and students even when these are removed from the school site at evenings, weekends and throughout holiday periods. This ensures constant visibility and mitigation of the safeguarding risk.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using school IT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual. For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person, such as Mr Henry, IT Technicians, a line manager or SLT.

Computer Viruses

At the Royal Liberty School, we discourage the use of memory sticks and external hard drives as they can be detrimental to the security of the network and data shared or

accessed. All files downloaded from the Internet, received via email or on removable media such as a memory stick should be checked for any viruses using school provided antivirus software before being used. Where possible Google drive should be used to save students work. Any USB or removable storage device which has sensitive or personal information on must be encrypted.

Never interfere with any antivirus software installed on school ICT equipment. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you on what actions to take and be responsible for advising others that need to know.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords that are not shared with anyone. The students are expected to keep their passwords secret and not to share with others. Staff and students are regularly reminded of the need for password security.

- All users read and agree to an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy.
- Users are provided with an individual network login username and cloud account. From Year 7 they are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If students think another person knows their password then they know how to reset it or they can ask their teacher or a member of the IT staff.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and VLE, such as the cloud and Google Apps, including ensuring that passwords are not shared and are changed regularly. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times.

Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password.

You must always keep your individual username and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and usernames should never be shared.

Staff and student initial/default passwords must be changed at first logon for all systems in school (this is enforced by software).

Strong password guidance will include the following:

- Passwords must be at least 8 characters (a-z, 0-9) in length (with upper and lowercase characters)
- Passwords must contain at least 1 number (0-9) and/or symbol eg ! * & # %
- Passwords must not be similar to your own name or username for example: cutler1

:
Google passwords must be at least 8 characters long (this is enforced by Google).

Other online systems accessed by staff and students may have their own password policy which they enforce. Where they are not enforced staff and students should follow the rules outlined above.

Managing the Internet
The Internet is an open communication medium, available to all. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the school network by students is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school students will have supervised access to internet resources (where reasonable) through the school's fixed and wireless internet technology.
- Staff will preview any recommended online services, software, sites and apps before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- School internet access is controlled through our web filtering service and other systems managed by the Network Manager, Ms Salmon.

- Students are aware that school-based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff discover an unsuitable site, the screen must be switched off and the incident reported immediately to the Network Manager or E-Safety Coordinator.
- If students discover an unsuitable site, the screen must be switched off and the incident reported immediately to the teacher.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up to date on all school machines.
- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up to date virus protection software. It is not the school's responsibility, nor the network manager's, to install or maintain virus protection on personal systems
- Students are not permitted to download programs on school-based technologies.
- If there are any issues related to viruses or antivirus software, the network manager should be informed via the call logging system for staff or via teachers for students.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly, both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Mobile and Wireless Technology

Many emerging technologies offer new opportunities for teaching and learning. Many existing mobile technologies such as tablets, gaming devices and mobile phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Devices

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes during the school day. At all times the device must be switched onto silent or off. (see mobile phone policy).
- The sending of inappropriate electronic messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Based Devices

- All staff and students must agree to the acceptable use policy before using any school based equipment, such as phones, tablets, Chromebooks, PCs and other devices.
- The sending of inappropriate electronic messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and tablets for off-site visits and trips, only these devices should be used.

Managing Email

- The school gives all staff and students their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students or parents, or conduct any school business, using any personal communication methods, e.g. email address, social networking, Twitter, video sites etc.

- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending sensitive emails to external organisations, parents or students are advised to cc or bcc their line manager if they think the issue might be contentious.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All email users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language, and not reveal any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission; they should virus check attachments.
- Students must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform the e-safety Coordinator and line manager if they receive an offensive email.
- Students are introduced to email as part of the ICT scheme of work in Year 7.
- All new members of the school community are shown how to use their email account when they join.

Safe Use of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness.

- Parents or carers must opt out if they do not want appropriate images of their child to be used within the school or on the website or for promotional material.
- Students must not take or distribute any images/audio/video of members of the school community.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

On a child's entry to the school, all parents/guardians will be asked to opt out if they do not wish their child's work/photos used for school related publications such as the school website, prospectus, news articles and other printed publications that the school may produce for promotional purposes. Parents/carers may withdraw permission, in writing, at any time. Email and postal addresses of students will not be published.

Managing Video Conferencing

Video conferencing or similar communications will be appropriately supervised for the students' age. All students are supervised by a member of staff when video conferencing. Students should ask permission from the supervising teacher before making or answering a video conference call. Parents must provide consent for their children to participate in video conferencing.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT, and associated risks.

- The policy and Acceptable Use Agreement on the school website.
- Parents/carers are required to provide consent to images of their child being taken/used in the public domain (e.g. on school website).
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
    - Website postings or Newsletter items
    - Emails and Communication

Review

This policy will be reviewed annually and amended as necessary.

Date of this policy: May 2018
Next review date: May 2019
Reviewed by: H.Desmond

Signature of Head Teacher:…… Date:……

Signature of Chair of Governors:…… Date:……

ACCEPTABLE USE POLICY: STAFF, GOVERNORS AND VISITORS

The Royal Liberty School - ICT Acceptable Use Policy / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff have to agree to the AUP everytime they logon. Any concerns or clarification should be discussed with Mr Henry, the school's E-Safety Coordinator.

- I understand that every time I login to a computer the AUP comes uop and I have to agree to the policy to be able to use the system.
- I will only use the school's email/internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 all electronic communications with students and staff are compatible with my professional role and will be done using the approved, secure school email system (initialsurname@royalliberty.co.uk).
- I will not give out my own personal details, such as mobile phone number and personal email address, personal Twitter account, or any other social media link including gaming account, to students.
- I will not share or discuss my professional role in any capacity when using social media, such as Facebook and Twitter, or anything else that could bring the school into disrepute.
- I will ensure that any private social networking sites/blogs etc that I create or actively contribute too are not confused with my professional role.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- Personal or sensitive data taken off site must be encrypted, e.g. on a password secured device or memory stick.
- I will not install any hardware or software without permission of Ms Salmon, the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of students and/or staff will only be taken, 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 will not use personal digital camera or camera phones for transferring images of pupils or staff without permission.
- 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 agree and accept that any computer/laptop or chromebook loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school’s E-Safety Policy and help students to be safe and responsible in their use of ICT and related technologies.
- I will not allow unauthorised individuals to access emails/internet/intranet or any data systems or LA systems
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that failure to comply with the AUP could lead to disciplinary action.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..……... Date ……

Full Name (printed):

Job title:

The Royal Liberty School

"Where boys are ambitious, where boys succeed"

ACCEPTABLE USE POLICY (AUP)

Acceptable Use Policy (AUP): Students, Parents / Carers

SCHOOL	
Reviewed by:	T Barrett (Business Manager)
Review Date:	May 2018

Next Review:	May 2019

Acceptable Use Policy (AUP): Students, Parents / Carers

Parent / Carers name:

……

Student name(s):

……

As the parent or legal guardian of the above student, I grant permission for my son to have access to use the Internet, Google for Education services (including Google mail) and other ICT facilities at school.

I know that my son has read and signed this agreement form and that he has a copy of the 12 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe, to prevent pupils from accessing inappropriate materials and to reduce the risk of exposure to radicalisation and extremism. These steps include using an educationally filtered service (E-Safe), restricted access e-mail, the use of classroom management software (RM Tutor), employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites he visits, and that if they have concerns about his e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my son's e-safety.

Parent /Carer signature:

……

Student signature:

……

Date: …… / …… / ……

ACCEPTABLE USE POLICY: STUDENTS

The Royal Liberty School - Student ICT Acceptable Use Policy