Online Safety Policy

Leadership Team Responsibility:	Simon Round, Sarah Morgan and Simon Beck
Version Date:	October 2018
Presented to Full Governing Body on:	14th November 2018
Review Date:	October 2020

Contents

What is Online Safety?

Information and Communications Technology (ICT) is now an essential education tool. With its benefits come dangers. This means we now have to think beyond the traditional school environment when ensuring every student's safety. Once the desktop computer was the only way to access the internet, now many mobile phones and games consoles offer broadband connections. Students now work online in school and at home and have personal devices not covered by network protection. Therefore the emphasis everyone needs to understand the risks and act accordingly.

Unfortunately though, there are times when Internet use can have a negative effect on children. Students, staff, parents and carers should be aware of the potential dangers and take measures to ensure safe usage of technology.

Introduction

ICT 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.

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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, internet technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Lister Community School we understand the responsibility to educate our students on Online Safety issues, teaching them 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. Both this policy and the Acceptable Use Agreements are inclusive of both fixed and mobile internet technologies provided by the school, such as PC's, laptops, personal digital assistants (PDAs), tablet PCs, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers, etc. and technologies owned by students and staff brought onto school premises, such as laptops, mobile phones etc.

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Imran Ahmed has been designated the role of Online Safety Co-ordinator within the school. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as London Borough of Newham, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by Simon Round (Deputy Headteacher) and Imran Ahmed (Online Safety Co-ordinator) 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 Policy for staff, governors, visitors and students, is to protect the interests and safety of the whole school community.

Online Safety skills development for staff

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Managing the school Online Safety message

- The Online Safety policy will be introduced to students at the start of each school year and to any students who join the school mid-phase.
- Online Safety posters will be prominently displayed in all classrooms.

Online Safety in the Curriculum

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

- Educating students on the dangers of technologies that may be encountered outside school is done as a specific unit within the ICT faculty. In addition the Online Safety curriculum will be covered by other curriculum areas with lessons where appropriate.

- 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 other 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, e.g. 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 teacher models, discussions and via the ICT curriculum.

Password Security

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

- All users read and accept an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.
- Users are provided with an individual network log-in. 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 you think your password may have been compromised or someone else has become aware of your password report this to the Online Safety Co-ordinator.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and data, Go4Schools and Realsmart learning portfolios, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Staff are advised to update their passwords every 30 days. RM Network passwords are reset each term.
- *Under no circumstances are staff allowed to let any other person to use their username and password. This could result in disciplinary action.*

Managing Online Safety within School

The internet is an open communication medium, available to all, at all times. 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.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites and materials before use.

- Staff will not avoid discussions and the research of terrorism as this may be relevant to the lesson being taught. Instead staff should consider appropriate guidance to ensure that the material being accessed is relevant and appropriate.
- Raw image searches are discouraged when working with students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research.
- 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.
- At present, the school endeavours to deny access to social networking sites to students within school.

Infrastructure

- In conjunction with RM, London Grid for Learning and Future Digital, the school has a monitoring system where web-based activity is monitored and recorded on all ICT equipment and school issued mobile phones.
- School internet access is controlled through the London Grid for Learning's web filtering service.
- Lister Community School is aware of its responsibility when monitoring staff communication under current legislation and takes into account the Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.
- Staff and 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 or students discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the class teacher.

Managing Online Safety outside of school

Web 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.

Students, Parents and Carers

- All students are advised to be cautious about the information given by others on sites. This is because other people may not be who they claim to be.
- Students, parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students, parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, school details, IM/email address and specific hobbies/interests).
- Students, parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students, parents and carers are asked to report any incidents of bullying to the school. Information leaflets are available in Reception.
- The school advises parents and carers to locate PC's and laptops in a highly visible part of the home, which can be regularly monitored.
- Students should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

School Staff

- If you are a member of a social networking site (e.g. Facebook) ensure that your security settings are high. If you need further advice on this matter see the RM Technician
- Staff who are members of social networking sites must not accept past and current students as friends for at least a period of 3 years after the student has left school and not before the student is 19 years of age. Please refer to Staff Guidelines for further information - Exceptions may be made in certain circumstances, such as a key worker wishing to maintain communication with a student who would otherwise have difficulty maintaining communication, but such cases are exceptional and should be discussed with either a Deputy Headteacher or Headteacher and agreement to this recorded.
- Staff are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- School laptops are only to be used by the staff member allocated the laptop. The laptop should not be used by family members and should only be used for work purposes and not for personal use.
- Under no circumstances should staff take any images and videos taken within the school environment off site without the authorisation of the Head Teacher or the delegated Deputy Headteacher, school issued mobile devices have been made available for such occasions where the taking of video or images are necessary to support the work of the school.

Mobile technologies (including mobile phones)

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smartphones 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.

Student Mobile devices

- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within the school day or on the school site. At all times the device must be switched onto silent.
- If a teacher has decided that student mobile phone use is necessary for a specific task within a lesson, then students will be clearly informed when and for what purpose they are permitted to use their mobile phone, and must only use the mobile phone for the identified period. The student must take responsibility for switching their phone back to silent after this period.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Staff Mobile Devices

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device except in the case of an emergency.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices

- The sending of inappropriate 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 laptops and PDAs for off site visits and trips, only these devices should be used.

Managing email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT Level 4 or above, Students must have experienced sending and receiving emails.
At Lister Community School:

- The school gives all staff 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 and if necessary email histories can be traced.
- Only the school provided email account should be used for school business.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform the Online Safety Coordinator/line manager if they receive an offensive email.
- Students are introduced to email as part of the ICT Scheme of Work.

Safe Use of Images and Film

Digital images are easy to capture, reproduce and publish and therefore could be misused. 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.With the written consent of parents (on behalf of students), the school permits the appropriate taking of images by staff and students with school equipment under the following guidance.
At Lister Community School:

Staff

- Staff must never take images or make videos of students covertly on any digital device
- Any images or videos that are made, must be for teaching and learning purposes.
- Staff that wish to take photographs or videos with their students as a keepsake, may do so in certain circumstances:
    - It should be declared to a senior member of staff;
    - The images / videos should never be taken covertly and always with the full consent of the students;
    - Should not be shared online or any social media account except for on official school media accounts, if in doubt to refer to the Assistant Headteacher with responsibility for Marketing;
    - Should always be appropriate and not used to undermine or embarrass a student.

Parents

- Will be allowed to film and take images of their child during performances but will be reminded at the beginning of any performance that any image or video taken must not be shared online or on any social media account as other students may also be included in such material.

Students

- Students are not permitted to use personal digital equipment, including mobile phones and cameras to record images of the students or staff within the school environment or when on field trips unless pre approved by a member of staff.

Publishing student's images and work

On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website.
- On the school's Learning Platform.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibitions promoting the school.
- General media appearances, e.g. local/national press to highlighting an activity, sent using traditional methods or electronically.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues etc. Parents/carers may withdraw permission in writing at any time. Email and postal addresses of students will not be published.

A potential risk of publishing student's images and work on the internet/ social media is that a child may become of interest to a sex offender. Locating people through the internet has become extremely easy, using widely available software, so if there is a picture and the name of a school, setting or youth group and the full name of the child or adult then it could be quite easy to find out someone's exact location or address which could then put them at risk. Therefore we at Lister Community School follow the procedure of never publishing a child's full name alongside their photograph.

Storage of Images

At Lister Community School:

- Images/films of children are stored on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously in order to comply with the Data Protection Act 1998.
At Lister Community School:

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher and implemented by the Deputy Headteacher for Assessment and the Data Manager.
- Any data taken off the school premises must be encrypted. (Advice must be sought from the RM Technician when doing this).

Copyright

The infringement of copyright is a criminal offence under the Copyright, Designs and Patents Act 1988 and could result in prosecution.
Just because something is on the web does not mean it is freely available for you to use in your own work. As with any material which is protected by copyright, you should seek the author's permission if you wish to use it. With text you can use up to 5% of any one piece of work without seeking permission. With images, sound, animations, and video clips, you should seek permission, unless you are specifically told you can download and use them freely.
Copyright law allows students special concessions but these are very limited. As a member of staff or a student you may use copyright material for your own personal study purposes only. This includes using copyright material as part of an assignment. If you later want to use the same material for any other purpose, you must seek permission.
You should always acknowledge the source of any 'third party' material you include in your own work.

Portable and Removable Storage Devices (RSD)

Over recent years, staff have increasingly needed to be fully mobile and connected, often taking information home or out of the school in order to maintain productivity and deliver services efficiently and effectively.
Staff should seriously consider whether the use of RSD, e.g. USB stick, is appropriate. Staff can access student data securely using CC4 Anywhere or through the Go4Schools website.
Data stored on a USB stick is, generally, not encrypted. ***Do not store sensitive information on a portable device. Advice on how to password protect your USB device can be obtained from the RM Technician.***

Child Protection

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to risk of harm. Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse children may pose as children to engage and then meet up with the young people they have been in communication with. This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones. An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Report to and discuss with the Online Safety Co-ordinator and the Safeguarding team in school and contact parents.
2. Advise the child on how to terminate the communication and attempt to save all evidence.
3. Contact Child Exploitation and Online Protection centre (CEOP) at www.ceop.gov.uk
4. Consider the involvement of police and social services.
5. Consider informing the Local Authority Online Safety officer, Lesley Craven.

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Cyberbullying Guidance

Cyberbullying is bullying through the use of communication technology like mobile phone text messages, emails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously.
- Making insulting comments about someone on a website, social networking site (e.g. MySpace) or online diary (blog).
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email.

Abusive language or images used to bully, harass, threaten another, whether spoken or written (through electronic means) may be libellous and may contravene the Harassment Act 1997 or the Telecommunications Act 1984. Within our School Behaviour Policy and Acceptable Use Agreement (Section 10), the use of the web, text messages, social media sites, email, video or audio to bully another student or member of staff will not be tolerated.
Bullying can be done verbally, in writing or images, including through communication technology (cyberbullying) e.g. graffiti, text messaging, email or postings on websites. It can be done physically, financially (including damage to property) or through social isolation.
Students and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

If a bullying incident directed at a student or member of staff occurs using email or mobile phone technology either inside or outside of school time:

- Advise the student/staff member not to respond to the message.
- Refer to relevant policies including Online Safety Policy, Acceptable Use Policy and Anti-bullying policy and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's email service provider.
- Notify parents of the children involved or in the case of a member of staff follow the incident reporting flowchart.
- Consider informing the police depending on the severity or repetitious nature of offence.
- Consider Informing the Head Teacher and LA Online Safety officer depending on the severity.

If malicious or threatening comments are posted on an Internet site about a student or member of staff

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Send all the evidence to appropriate point of contact via the Online Safety incident flowchart.
- Endeavour to trace the origin and inform police as appropriate.
- Consider informing the Head Teacher or LA Online Safety officer (Lesley Craven).

Misuse and Infringements

Any misuse of computer equipment or mobile technology that breaches any of the guidelines set out in the Online Safety policy should be reported to the Online Safety Co-ordinator. Should an infringement of the school's Acceptable Use Agreement, Online Safety Policy or Removal Storage Device Policy occur, please report it to Simon Round, Deputy Headteacher.

Students found to be in infringement of this policy will be subject to sanctions as outlined the Behaviour Policy. Staff may be subject to disciplinary action.

Complaints

Complaints relating to Online Safety should be made to Imran Ahmed (Online Safety Coordinator), Simon Round (Deputy Headteacher) or the Anthony Wilson (Headteacher) at the following address:

Lister Community School
St. Mary's Road,
Plaistow,
London
E13 9AE

Inappropriate material

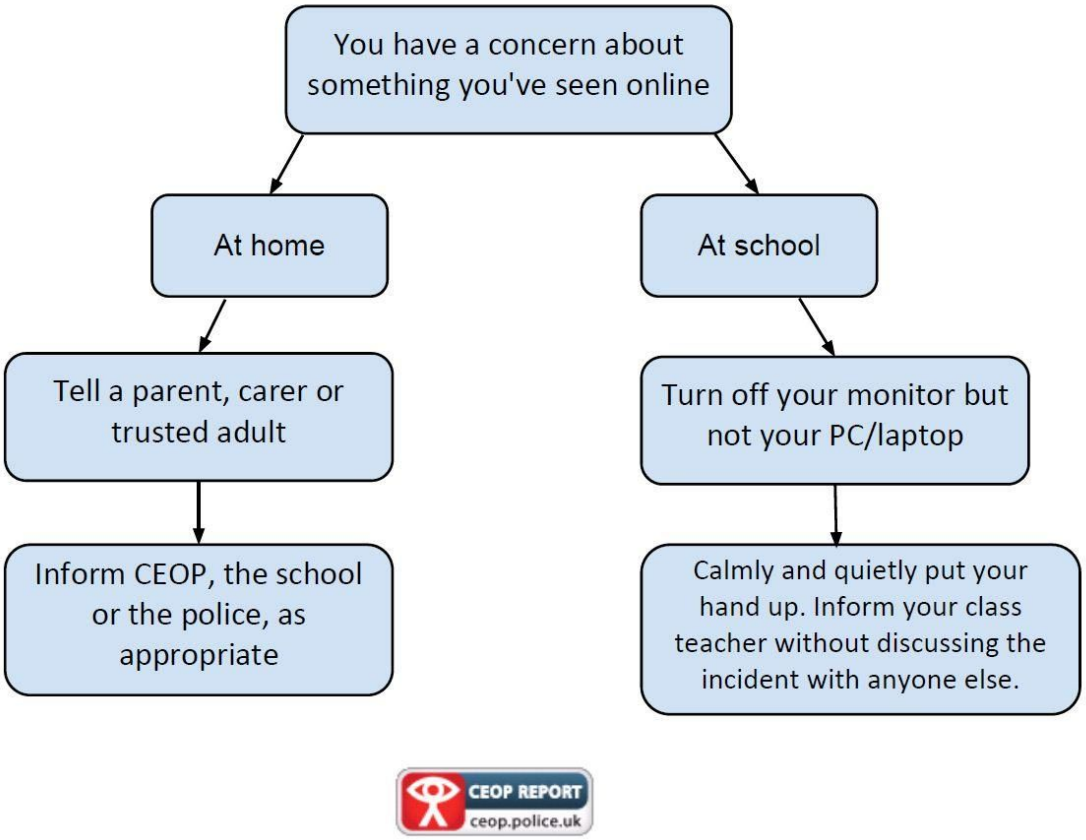
At Lister Community School:

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported and follow Online Safety incident flowchart.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the teacher or Imran Ahmed, Online Safety Coordinator depending on the seriousness of the offence.
- Serious infringements may result in investigation by the Head Teacher/LA and could lead to immediate suspension, possibly leading to dismissal and involvement of police.

Equal Opportunities

The school endeavours to create a consistent message with parents and carers for all students and this in turn should aid establishment and future development of the schools' Online Safety policy.
However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.
Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Student Flow Diagram



Staff Flow Diagram