Roman Road Primary School

The Acceptable Use of the Internet and related Technologies

John Gordon / Mohammed Wadud / Kim Eldridge

Updated September 2021

To Review – September 2022

Contents

- Overview
- Whole school approach
- Roles and responsibilities
- Communications pupils, staff and parents
- Complaints procedure
- How we manage e-mail
- Managing the Internet Safely
- Use of digital and video images
- Parent / Pupil Home School Agreement
- E-safety Complaints, allegations, disclosures form

(Linked to Anti Bullying Policy, Anti Cyberbullying Policy, Code of Conduct Policy, Staff Acceptable Use agreement, Safeguarding Policy, DFE Keeping Children Safe in Education 2018, Behaviour Policy, ICT Policy, Home-school agreement, Complaints procedure)

Overview

Policy: The Acceptable Use of the Internet and related Technologies

Our e-Safety 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. It will be reviewed annually.

This policy is equally applicable to all members of staff working in Key Stage one, Key Stage two, Reception, Nursery, and two year old provision.

This policy sets out the extent to which information and communication technology (ICT) capability and other key skills enable learners to improve the quality of their work and make progress. The extent to which learners adopt safe and responsible practices in using new technologies, including the Internet. We have a duty to ensure that all students are able to make a valuable contribution to society & this is impossible to achieve if we do not ensure that students develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

Effective and safe use of digital resources - Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

'The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners'.

The DFE publication Keeping Children safe in Education 2016 and the provisions of the *Children Act 2004*[1], *Working Together to Safeguard Children*[2] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation

- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in our 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.

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – accessing websites using Google Chrome, Microsoft Edge, Safari
- Social media apps including the most common ones which are WhatsApp, Facebook, Instagram, Snapchat, and Tiktok
- Live streaming using YouTube or other media apps
- Online vlogging – YouTube channel
- Video calls
- Blogs (an on-line interactive diary)
- Mobile phones with camera and video functionality
- Online gaming community – enabling users to connect and chat, go on live streams
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

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

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 Head Teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

E-Safety Co-ordinator: John Gordon
(In his absence Sam Stone or Leisa Adams)
ICT Co-ordinator: Kim Eldridge
IT Network Manager: Mohammed Wadud

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP)[3]. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [4] on e-Safety and are updated at least annually on policy developments.

[3] http://www.ceop.gov.uk/
[4] Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

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 pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication 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 pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.

Schools should include e-safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to contrail and minimise online risks and how to report a problem.

Schools should ensure that they make efforts to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned an e-safety/AUP form.

How will the policy be introduced to pupils?

Each term we have an e-safety refresher session delivered to all pupils where it highlights all the key areas on how to stay safe online, as well as discussion on any new technology and information to create awareness. During this session, the school e-safety is shared, informing all pupils, the expectations and responsibilities ensuring that the policy is followed correctly.

Possible statements:

- All pupils should be aware that all activity on the Internet is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- All pupils should be made aware of protecting personal information – not sharing passwords to access the school systems, google accounts.
- All pupils will be made aware of the school's filtering system and that they should not be attempting to access or search online anything that is against school policy.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

Possible statements:

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that 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.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

Possible statements:

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Age requirement to use social media apps, highlighting most common apps where the age is set to 13 years old and for WhatsApp it is 16 years old.
- To ensure web filtering is requested to their ISP to ensure browsing the net at home is safe and children are protected from explicit web content.
- Keeping parents up to date with new technology and social media apps.

How will complaints be dealt with

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.

Sanctions for pupils:

- Interview or discussion with teacher / Learning mentor / councillor /e-Safety Coordinator / Head Teacher;
- school consequence system
- 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.

Sanctions for staff: Depending on the severity of the infringement, the school will follow London Borough of Newham disciplinary procedures, which may consist of:

- A timely word (informal)
- Written warning (formal)
- Final written warning
- Dismissal

Bodies that may be referred / reported to:

- Newham LADO
- Newham Human Resources
- Police

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Complaints of cyberbullying 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.

How we manage email

Students are encouraged to use their school approved email account only when communicating about school related issues. They should regard this as their professional profile; the school email address should only be used for educational purposes.

Students must immediately tell a teacher if they receive offensive email. Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Excessive social email use can interfere with learning and is an abuse of the system. Email sent to external organisations should be written carefully and authorised by the relevant member of staff before sending, in the same way as a letter written on school headed paper. The forwarding of chain messages is not permitted.

Managing the internet safely

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

 access to world-wide educational resources, including museums and art galleries;
 access to experts in many fields for pupils and staff;
 educational and cultural exchanges between pupils world-wide;
 collaboration between pupils, professionals and across sectors;
 access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

 communication systems;
 improved access to technical support, including remote management of networks and automatic system updates;
 online and real-time ‘remote’ training support;
 secure data exchange between local and government bodies.
network.

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the

Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Use of digital and video images

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website.

Take care when using photographs or video footage of pupils on the school website. Consider using group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

· If the pupil is named, avoid using their photograph / video footage.
· If the photograph /video is used, avoid naming the pupil.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise. If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. If showcasing examples of pupils work consider using only their first names, rather than their full names.

Only use images of pupils in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken. Parental permission should be obtained before publishing any photographs, video footage etc of pupils on the school website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the school; a printed copy of the specific image should be attached to this form. A Parental Permission Form is an appropriate way of achieving this.

Procedures: Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory.

Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If the school's website contains any guestbook, noticeboard or blog, they need to be monitored to ensure they do not contain personal details of staff or pupils.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Digital images – it is very easy to record or take phones using mobiles. It is very important that such capture are then not posted on social media sites or shared.

Technical:
Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school. When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web. [An ALT

tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers] Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.
There are safe online environments for publishing, such as the LGfL portal or Learning Platform and School 'Book Publishing' websites.

Education:
Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

Policy statements:
In this school:
* The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
* Uploading of information is restricted to the IT Manager (Mohammed Wadud)
* 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 will not be published;
* Photographs published on the web do not have full names attached;
* 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;
* Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
* We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
* We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
* Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
* Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school;
* Pupils 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;

Pupils are taught about how images can be abused in their eSafety education programme;

Parent / Pupil Home School Agreement

Social Networking - The school wishes to remind its parents that Facebook and other Social Medias are only intended for users aged over 13. The school also understands that it is very easy for young people (or indeed adults) to enter an incorrect date of birth or false information to open an account. In fact, according to Ofcom's UK Media Literacy report (April 2011) "social networking continues to increase and 47% of 10 – 12 year olds have a active profile". Concerns have been raised over some of the possible issues including:

- Interaction between teachers and pupils or parents.
- Inappropriate communications between colleagues.
- Unpleasant or abusive postings about teachers or pupils.
- Criticism of the school (not personally abusive).
- The setting up of fake profiles

Any form of misuse directed at the school, its employees, the pupils or anyone associated with the school will be taken very seriously. If any illegal activity or content is suspected the school will inform the necessary authorities.

Pupils and Parents are requested to sign the Home School Agreement form to show their support of the school in this important aspect of the school's work

The school advices:

- You should ensure that adequate parental control settings are applied to your home Internet
- It is important to talk to your children about staying safe on line and that they know they can turn to you if they get in any difficulty
- Social media sites have reporting facilities to report misuse or abuse
- Monitor the amount of time and which web sites your child is accessing
- Situate the technology devises in a family area
- Be aware that if your child is taking their devise out of the home they could connect to public wifi
- Look out for the friendly wifi symbol which shows that the wifi has filters in place to limit access to inappropriate content

John Gordon / Mohammed Wadud / Kim Eldridge
September 2021

Signed by School Governors:

To Review September 2022

E- Safety – Complaint, Disclosure or Allegation about Staff misuse

Report to be made to either HT or DHT (e-Safety lead)

Nature of E-Safety Infringement – all details relating to infringement including time, place, name of member of staff, full description of infringement
Action taken by HT / DHT (E-Safety lead)
Signature: (or tick if wavered): HT / DHT signature: Date