RICHARD COBDEN
PRIMARY SCHOOL

Online Safety Policy

Contents

1 ONLINE SAFETY: THE ISSUES

1.2 Introduction

Nowadays, children are “digital natives”, growing up in a world dominated by information and communications technology (ICT) that provides them with access to a wide range of information and increased opportunities for instant communication and social networking.

Using the internet can benefit children’s education and give them more opportunities to socialise, but it can also present several risks. Children are often unaware that they are as much at risk online as they are in the real world, and parents and teachers may not be aware of the actions they can take to protect them.

In the face of these risks, parents and schools may deal with the problem by denying or limiting access to the internet; however, this may have little effect as children can access the internet in a range of localities such as libraries, internet cafes and on mobile phones.

It is Camden’s policy that the educational and social benefits of the internet should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, schools need to develop an Online Safety strategy working in partnership with parents.

This document provides schools with guidance to achieve this by helping them to recognise the risks and take action to help children use the internet safely and responsibly.

1.2 Information on technologies

Internet technology provides a wide range of activities, including access to information, electronic communications and social networking; each has a clear educational use but also inherent risks for children. The table shown at appendix 5 provides brief details of the various uses of the internet together with their benefits and risks.

1.3 Benefits of ICT

Use of ICT is so universal that it is of huge benefit to children to learn these skills in order to prepare themselves for the working environment; it is important that teachers are aware that the inherent risks are not used to reduce children’s use of ICT.
The internet can make a huge contribution to children’s education and social development by:

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence

- improving pupil’s research and writing skills

- allowing children with disabilities to overcome communications barriers

- enabling children to be taught "remotely", for example children who are unable to attend school

- improving pupil's wellbeing through the social and communications opportunities offered

- providing access to a wide range of educational materials and teaching resources.

1.4 Risks

The risk associated with use of ICT by children can be grouped into 4 categories.

1.4.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.4.2 Contact

Chat rooms and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as cyber bullying. More details on this can be found in section 4.5 of this policy.

1.4.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.

1.4.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people

- using information from the internet in a way that breaches copyright laws

- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience

- cyber bullying (see section 4.5 for further details).

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.

1.5 Key contacts

Richard Cobden Primary School
29 Camden Street
NW1 0LL

Name of school/college:

Headteacher:
Name: Kathy Bannon
Contact via school admin e-mail: admin@rcobden.camden.sch.uk

Online safety co-ordinator:
Name: Alvaro Scrivano
Contact via school admin e-mail: admin@rcobden.camden.sch.uk

Nominated LGfL contact:
Name: Alvaro Scrivano
Contact via school admin e-mail: admin@rcobden.camden.sch.uk

Designated safeguarding lead:
Name: Maria Shurety
Contact via school admin e-mail: admin@rcobden.camden.sch.uk

Nominated governor:
Name: Deborah Isaacs
Contact details: d.isaacs@rcobden.camden.sch.uk

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO):
Name: Sophie Kershaw
Contact details: 020 7974 4556

Child and Family Contact/MASH team:
Manager: Jade Green
Tel: 020 7974 1553/3317
Fax: 020 7974 3310

Camden online safety officer:
Name: Jenni Spencer
Tel: 020 7974 2866

Prevent Education Officer
Name: Jane Murphy
Tel: 020 7974 1008

Prevent Education Officer
Name: Jane Murphy
Tel: 020 7974 1008

2 SCHOOL ONLINE SAFTEY STRATEGIES

2.1 Purpose and Description

Computing is now a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Schools should have an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

2.2 Elements of Online Safety

Schools can enable an “e-safe” environment for pupils by ensuring that the following aspects are addressed.

2.2.1 Safe systems

Most Camden schools are linked to the internet via IT, the London Grid for Learning platform. Camden’s Schools IT team ensures that IT offers a safe e-learning environment by providing filtering software to block access to unsuitable sites, anti-virus software and internet monitoring systems.

2.2.2 Safe practices

Schools need a strong framework of Online Safety policy and practice that ensures everyone is aware of the issues and knows what is expected of them in terms of their own acceptable use of the internet and other technologies. Online Safety policies should be consistent with related school policies such as anti-bullying and behaviour.

2.2.3 Safety awareness

It is vital that children are able to keep themselves and others safe and use the internet responsibly. Schools, working in partnership with parents and carers, have an important role in raising pupils’ awareness of the potential dangers of using the internet and helping them to develop their own strategies to avoid these risks and keep safe on-line.

Because many children will have access to the internet at home, schools need to ensure that parents and carers are fully aware of Online Safety issues so that they can extend Online Safety strategies to the home environment.

2.3 Roles and responsibilities

A successful Online Safety strategy needs to be inclusive of the whole school community and forge links with parents and carers. The strategy must have the backing of school governors, should be overseen by the head teacher and be fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Head teacher’s role

Head teachers have ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school’s online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote online safety and forward the school’s online safety strategy

- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

2.3.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the head teacher in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

2.3.3 Online Safety contact officer's role

All schools should have a designated online safety co-ordinator who is responsible for co-ordinating online safety policies on behalf of the school. Ideally, the officer should be a senior member of the management team. Given the issues associated with online safety, it is appropriate for the designated safeguarding lead to be the school's online safety co-ordinator.

The online safety co-ordinator should have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's online safety policy
- ensure that staff and pupils are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- ensure that all staff and pupils have read and signed the acceptable use policy (AUP)

- report annually to the board of governors on the implementation of the school's online safety strategy
- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues to Camden's online safety officer.

In addition, it is an Ofsted recommendation that the online safety co-ordinator receives recognised training CEOP or E-PICT in order to carry out their role more effectively. In Camden, this is available from the CLC.

2.3.4 IT manager's role

- the maintenance and monitoring of ICT, including anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to a member of the Senior Management Team.
- supporting any subsequent investigation into breaches and preserving any evidence.
- The ICT Manger is the Online Safety Contact officer.

2.3.5 Role of school staff

Teaching staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's Online Safety and acceptable use policy and procedures
- communicating the school's Online Safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using IT
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the Online Safety contact officer
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the Online Safety contact officer.

2.3.6 Designated safeguarding lead

Where any Online Safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the school who will decide whether or not a referral should be made to Safeguarding and Social Care or the Police. In some schools, the designated child protection teacher will be the Online Safety contact officer.

2.4 Pupils with special needs

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on Online Safety practice as well as closer supervision.

SEN co-ordinators are responsible for providing extra support for these pupils and should:

- link with the Online Safety contact officer to discuss and agree whether the mainstream safeguarding systems on IT are adequate for pupils with special need.
- where necessary, liaise with the Online Safety contact officer and the Schools IT team to discuss any requirements for further safeguards to IT or tailored resources and materials in order to meet the needs of pupils with special needs
- ensure that the school's Online Safety policy is adapted to suit the needs of pupils with special needs.
- liase with parents, carers and other relevant agencies in developing Online Safety practices for pupils with special needs
- keep up to date with any developments regarding emerging technologies and Online Safety and how these may impact on pupils with special needs.

2.5 Working with parents and carers

It is essential that schools involve parents and carers in the development and implementation of Online Safety strategies and policies; most children will have internet access at home and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue Online Safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The head teacher, board of governors and the Online Safety contact officer should consider what strategies to adopt in order to ensure parents are aware of Online Safety issues and support them in reinforcing Online Safety messages at home.

Parents are provided with information on ICT learning and the school's Online Safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. The school offers regular Online Safety sessions to parents and carers delivered by the school's CEOP Ambassador, Mr Alvaro Scrivano. Mr Scrivano is also available when parents and carers have a concern about their child's use of technology. The CSCB online safety leaflet for parents is also be available on the school website: link

3 ONLINE SAFETY POLICIES

3.1 Accessing and monitoring the system

- Access to IT in primary schools should be via a class log-in and password.
- The Online Safety contact officer should keep a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.
- Network and technical staff responsible for monitoring systems should be supervised by a senior member of their management team.
- The Online Safety contact ext. 34 and teaching staff should carefully consider the location of computer terminals in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.
- Staff should be required to change their password every 6 months.

3.2 Confidentiality and data protection

- The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 1998. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.
- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School. Any breaches of data security should be reported to the head teacher immediately.
- Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.

3.3 Acceptable use policies

- All IT users within the school will be expected to sign an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the school Online Safety rules regarding their internet use.

- For primary school pupils, acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to IT in school (see appendix 1).

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 3).

The Online Safety contact officer will keep a copy of all signed acceptable use agreements.

3.3 Teaching Online Safety

Department of Education guidance Teaching online safety in schools available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

3.3.1 Responsibility

One of the key features of the school's Online Safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the online safety co-ordinator, but all staff should play a role in delivering online safety messages.
- The online safety co-ordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.
- The online safety co-ordinator should ensure that any external resources used for teaching online safety have been thoroughly reviewed in advance.
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the wider curriculum.
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Teachers may wish to use PSHE lessons and during statutory relationships and sex education as a forum for discussion on online safety issues to ensure that

pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- Schools should teach online safety in a safe environment that allows pupils to discuss issues in an open, honest and non-judgemental way and it is recommended that the designated safeguarding lead is involved in the development of any lessons teaching online safety.
- As these discussions may lead to pupils recognising that they have been harmed online, teachers should be aware that following discussions, pupils may wish to make a disclosure
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.

.

3.3.2 Content

- The teaching of online safety should focus on:
- how to critically evaluate and make judgements on online content
- how to recognise techniques used to persuade or manipulate, for example extremist views, grooming and targeted marketing
- what is and is not acceptable online behaviour
- identifying online risks
- how to get help and support.

Pupils should be taught all elements of online safety included in the curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- are responsible, competent, confident and creative users of information and communication technology.

Teaching online safety should enable pupils to:

- understand the specific harms and risks inherent in using the internet, for example how people can behave differently on the internet and how the internet can be used to magnify and distort information and provide a platform for "fake news" and extremist views;
- how to stay safe online, how to identify online harm and abuse and what actions to take report this.

3.3.3 Delivering Online Safety messages

- Teachers are primarily responsible for delivering an ongoing Online Safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.

- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers may wish to use PSHE lessons as a forum for discussion on Online Safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

- Teachers should ensure that the school's policy on pupils' use of their own mobile phones in school is adhered to.

3.4 ICT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.

- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased.

- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with pupils regarding school work, this should be via IT and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.

- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5.3 Exit strategy

- When staff leave, their line manager should liaise with the network manager to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

3.5 Staff training and conduct

3.5.1 Training

- All school staff and governors should receive training with regard to IT systems and online safety as part of their induction and this should include a meeting with the online safety co-ordinator and the network manager.

- Staff should also attend specific training on online safety available from the CSCB so that they are aware of the risks and actions to take to keep pupils safe online. School management should ensure that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

Camden City Learning Centre offers whole school training including updates as well as training for governors and parents.

3.5.2 IT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils. Staff should refer to the model social media policy for school staff for further guidance.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.

- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images on personal mobile devices erased.

- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff should be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.

- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with pupils regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.

- When making contact with parents or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts such as SN should never be used.

- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops or i-pads provided by the school, they must ensure the equipment is kept safe and secure at all times.

3.6 Safe use of ICT

3.6.1 Internet and search engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.

- Primary school children should be supervised at all times when using the internet.

- Pupils should not be allowed to aimlessly “surf” the internet and all use should have a clearly defined educational purpose.

- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the Online Safety contact officer, who will liaise with the Schools IT team for temporary access. Teachers should notify the Online Safety contact officer once access is no longer needed to ensure the site is blocked.

3.6.2 Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author’s view is objective and what authority they carry

- carrying out comparisons with alternative sources of information

- considering whether the information is current and whether the facts stated are correct.

In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

3.6.3 Emails

IT hosts an email system that allow pupils to send emails to others within the school or to approved email addresses externally.

- Access to and use of personal email accounts on IT is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

- Emails should only be sent via IT to addresses within the school system or approved external address.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the Online Safety contact officer who will liaise with the Schools IT team.

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.

- All email communications should be polite; if a pupil receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- Users should be aware that as use of e-mail via IT is for the purposes of education or school business only, and all emails may be monitored.

- Access to email systems by primary school pupils should be via a class email address only.
- All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

3.6.4 Social networking sites, newsgroups and forums

Social networking sites such as Facebook, MySpace and Bebo allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

- Access to unregulated public social networking sites, newsgroups or forums should be blocked.

- Where schools identify a clear educational use for these sites for on-line publishing, they should only use approved sites such as those provided by the London Grid for Learning via IT.

- Any use of these sites should be strictly supervised by the responsible teacher.

- Pupils should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- In order to teach pupils to stay safe on social networking sites outside of school, they should be advised:

    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted

    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them

    - to behave responsibly whilst on-line and keep communications polite

    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.6.5 Chat rooms and instant messaging

Chat rooms are internet sites where users can join in "conversations" on-line; instant messaging allows instant communications between two people on-line. In most cases, pupils will use these at home although IT does host these applications.

- Access to public or unregulated chat rooms will be blocked except for the site hosted by IT, which is to be used for educational purposes only.

- Pupils should be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- In order to teach pupils to stay safe whilst using chat rooms outside of school, they should be advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
    - only use moderated chat rooms that require registration and are specifically for their age group
    - not to arrange to meet anyone whom they have only met on-line
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.6.6 Video conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- Video conferencing should only be carried out using approved software via IT. These can be booked in via http://cms.lgfl.net/lgfl/we/vc.

- Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the Schools IT team.

- Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call.

- Teachers should ensure that pupils are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.

- Photographic or video devices may be used by teachers only in connection with educational activities including school trips.

- Photographs and videos may only be downloaded onto the school's computer system with the permission of the network manager and should never enable individual pupils' names or other identifying information to be disclosed.

3.6.7 School website

- Content should not be uploaded onto the school website unless it has been authorised by the Online Safety contact officer and the head teacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- Schools should designate a named person or persons to have responsibility for uploading materials onto the website.
- To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website.
- Children's full names should never be published on the website.
- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.6.8 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Children's names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

3.6.9 Pupils own mobile phone/handheld systems

The majority of pupils are likely to have mobile phones or other equipment that allows them to access internet services, and these can pose a major problem for schools in that their use may distract pupils during lessons and may be used for cyber bullying.

However, many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to.

Schools will need to give serious consideration as to the policy regarding use of pupils' own equipment on school premises. Generally, use of mobile phones or other equipment should be forbidden in classrooms but schools may wish to allow pupils to use mobile phones during breaks.

3.6.19 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Children's names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

- Staff should not use personal devices to take photographs of pupils.

- Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

4 RESPONDING TO INCIDENTS

4.1 Policy statement

- All incidents and complaints relating to Online Safety and unacceptable internet use will be reported to the Online Safety contact officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the Online Safety contact officer on the Online Safety incident report form (appendix 4).

- A copy of the incident record should be emailed to Camden's designated Online Safety officer at jenni.spencer@camden.gov.uk.

- Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action. Incidents involving the headteacher should be reported to the chair of the board of governors.

- The school's Online Safety contact officer should keep a log of all Online Safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's Online Safety system, and use these to update the Online Safety policy.

- Online Safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.

Although it is intended that Online Safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the Online Safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the Online Safety contact officer and details of the website address and URL provided.

- The Online Safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (eg: sex education) that they notify the Schools IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

4.3 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

- The incident should be reported to the Online Safety contact officer and details of the website address and URL recorded.

- The Online Safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of ICT by staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the head teacher and the Online Safety contact officer immediately.

- The Online Safety contact officer should notify the network manager so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the Online Safety incident report form.

- The Online Safety contact officer should arrange with the network manager or Schools IT team to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.

- If the materials viewed are illegal in nature the head teacher should report the incident to the police and follow their advice, which should also be recorded on the Online Safety incident report form.

4.5 Online bullying

4.5.1 Definition and description

Traditionally, bullying took place face to face in the physical world; on-line, bullying can take on a new dimension with technologies such as email, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text

- posting insulting, derogatory or defamatory statements on blogs or social networking sites

- setting up websites that specifically target the victim

- making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping").

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies should cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of cyber bullying should be reported to the Online Safety contact officer who will notify record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone’s life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of Online Safety awareness and education, pupils should be told of the “no tolerance” policy for cyber bullying and encouraged to report any incidents to their teacher.

- Pupils should be taught:

    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.

- Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully’s access to the site can be blocked.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Online bullying of school staff

- Head teachers should be aware that teachers may become victims of cyber bullying by pupils *and/or their parents*. Because of the duty of care owed to staff, head teachers should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils *and parents*.

- The issue of cyber bullying of teachers should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.

- Incidents of cyber bullying involving teachers should be recorded and monitored by the Online Safety contact officer in the same manner as incidents involving pupils.

- Teachers should follow the guidance on safe ICT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.

- Personal contact details for teachers should not be posted on the school website or in any other school publication.

- Teachers should follow the advice above on cyber bullying of pupils and not reply to messages but report the incident to the head teacher immediately.

- *Where the bullying is being carried out by parents the head teacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.*

4.6 Sexting and sexual abuse and harassment by peers

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases, these actions may be harmful or abusive or may constitute harassment or online bullying.

“Sexting” or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Schools also need to be aware of the issue of “up-skirting” where pictures are taken of under a person’s clothing without them knowing in order to view their genitalia or buttocks with a view to sharing the images in order to distress or humiliate the victim. This is now a criminal offence.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Schools need to be aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this.

On-line behaviour that involves sexual abuse and bullying is a criminal offence, although it is unlikely that the perpetrator will be prosecuted where it is a peer of the victim.

However, schools need to include responses to sexual bullying in their behaviour policy and make a referral to Children's Safeguarding and Social Work for any pupil who displays sexually abusive behaviour towards other pupils. Staff should refer to Camden's "Children who harm other children" guidance for further details on this. http://www.cscb-new.co.uk/downloads/policies_guidance/local/Children%20who%20harm%20other%20children%20protocol.pdf

Schools need to be aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this.

Schools should be aware of the duty under statutory guidance Keeping children safe in education and Sexual violence and sexual harassment between children in schools and colleges which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCB Sexually harmful behaviour protocol for further details. https://cscb-new.co.uk/?page_id=8266.

Schools should be aware of the duty under statutory guidance Keeping children safe in education and Sexual violence and sexual harassment between children in schools and colleges which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCP Sexually harmful behaviour protocol for further details. https://cscp.org.uk/resources/sexual-harmful-behaviours/

Schools should also be aware of when any of these behaviours may be linked to the sexual exploitation of a pupil or is being carried out as a gang-related activity. Staff should refer to the CSCB child sexual exploitation guidance for further details. http://www.cscb-new.co.uk/wp content/uploads/2015/09/Multi_Agency_Guidance_On_Child_Sexual_Exploittion_2015.pdf

4.7 Risk from inappropriate contacts with adults

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

- All concerns around inappropriate contacts should be reported to the Online Safety contact officer and the designated child protection teacher.

- The designated child protection teacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The designated child protection teacher can seek advice on possible courses of action from Camden's Online Safety officer in Safeguarding and Social Care.

- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated child protection teacher and the Online Safety contact officer should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school ICT equipment or networks, the Online Safety contact officer should make a note of all actions taken and contact the network manager or Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.8 Social Media Guidelines

- Social media include all forms of online media that can be accessed by a wide audience from anywhere. They include but are not limited to such sites as Facebook, Twitter, LinkedIn, Issuu, Flickr, Vimeo, Youtube, and Instagram, for instance. They also include websites, messaging boards, discussion forums, and blogs. In other words, any form of online media that can be accessed by the general public is included in this definition.

- At all times Online Safety Policy and Guidelines regarding Social Networking with Children and Young People are to be observed by all.

- Use of social media should be treated in exactly the same way as any interaction with the mass media. In other words, treat all content as you would a press release or a public statement. Anything which is broadcast in your capacity as member of school staff must be accessible to the school's Headteacher.

- Richard Cobden Primary School respects the right of school personnel to express views on their personal social media sites. However, you should not (on either your open or restricted social media) publish personal (e.g. derogatory, defamatory or offensive) comments, information and/or pictures about colleagues or pupils your work for in connection with your work for the school.

- School staff are reminded of their responsibility 1.to recognise the integrity of the school's teaching on the curriculum and moral values, 2.to respect the dignity of persons, 3.to acknowledge the special role of teachers 4. to promote the common good of human beings applies always and everywhere including on personal media sites.

- School staff who proffer opinions on any topics related to Education on their personal media should specifically state that their views are entirely their own. Personal sites may not carry school logos and school job titles may not be used as primary headings on personal sites. Where, in the judgement of the Headteacher, the content of a personal social media site is deemed to be in danger of causing reputational damage to the school, the individual may be required to remove any indication of their school connection on their personal social media and may be requested to remove the content

4.9 Risk from contact with violent extremists

- Many extremist groups who advocate violence use the internet as a means of developing grievance, promoting extremist thought and division. They can use this to justifying verbal or physical violence against another group. Terrorist groups may also use the internet and social media to provide information on preparing explosives or carrying out terrorist acts. Some young people may be particularly vulnerable, lack resilience and so be more susceptible to these influences and may be radicalised as a result.
- The Prevent Duty requires all schools to prevent young people from being radicalised and drawn into terrorism. Schools need to consider how their leadership and management, school ethos and curriculum including online safety supports with building children's resilience to any radicalising influences. All Local Authorities are required to have a Channel Panel which offers a voluntary support package to individuals who have been referred due to a particular vulnerability. This is a multi-agency panel with a variety of interventions on offer to the to encourage critical thinking, stop the radicalisation process and divert them from extremism

- All school staff who use the internet as part of their lessons need to be aware of their responsibilities to promote good conduct, support young people to be aware of the dangers of contact and how to put security in place and how to recognise and report inappropriate content. This is part of building young people resilience which is one of the 6 strands of the Prevent Duty.
- Staff need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation.
- Pupils and staff know of the risks of becoming involved in groups with extremist ideologies and the tactics they may to groom and exploit. Staff and young people should also be made aware that accessing and sharing certain content is against school policies and certain contact with certain groups is illegal.
- The school should ensure that adequate electronic filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism. Schools also need to ensure that other filtering methods are in place, e.g. consideration of how the internet is accessed in school and which staff are available to support. Also children should be able to support one another to filter content and report concerns they have for each other.
- All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.
- The online safety co-ordinator and the designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer to MASH. If there is imminent danger dial 999. In all other circumstances follow the schools safeguarding procedures by speaking to the DSL. If next steps are not clear speak to the Prevent Education Manager or refer directly to MASHadmin@camden.gov.uk
- Schools may contact the Prevent Education Manager for advice on any of the above.
- Further information is available in the CSCP guidance “Safeguarding children and young people from radicalisation and extremism” available at: https://cscp.org.uk/resources/radicalisation-and-extremism-resources/

4.10 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- *The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.*

- *Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor*

- *Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.*

5 SANCTIONS FOR MISUSE OF SCHOOL ICT

Individual schools are responsible for deciding what sanctions will be applied for breach of acceptable ICT use policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors. The following is a framework recommended by LGfL that schools may want to adopt: For each point, schools may record their own detailed list of breaches and corresponding sanctions.

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions could include referral to the class teacher or tutor as well as a referral to the Online Safety contact officer.

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of Online Safety policy that are non-deliberate, such as:

- continued use of non-educational sites during lessons
- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to class teacher or tutor
- referral to Online Safety contact officer
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

5.1.3 Category C infringements

These are deliberate actions that either negatively affect IT or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to class teacher or tutor
- referral to Online Safety contact officer
- referral to head teacher
- loss of access to IT for a period of time
- contact with parents
- any sanctions agreed under other school policies

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's Online Safety officer.

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the head teacher who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on IT and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking

- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Possible sanctions include:

- referral to the head teacher
- removal of equipment
- referral to Camden's Online Safety officer
- referral to SSC or police
- suspension pending investigation
- disciplinary action in line with school policies

Effective From	September 2020
Review Date	September 2023

Appendix 1

Online Safety Agreement for pupils

These rules will help us to stay safe when using ICT at school:

1. I cannot use school ICT equipment until my parent/s have signed my use agreement form and the completed form has been returned to school.

2. I can only use the computers and other ICT equipment for my schoolwork and only with my teacher's permission.

3. I can only go online or use the Internet at school when a teacher gives permission and an adult is present.

4. If there is something I'm not sure about I will ask my teacher.

5. I will not use the Internet, email, mobile phones or any other ICT equipment to be mean, rude, or unkind about other people.

6. I will not tell anyone my password.

7. If I find anything that upsets me, is mean or rude, or things I know are not acceptable at our school, I will not show others, I will turn off the screen and get a teacher straight away

8. I must not bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, USB drives and software.

9. I will ask my teacher's permission before I put any personal information online.

Personal information includes:

□ Name

□ Address

□ Email address

□ Phone numbers

□ Photos

□ School's name

10. I will be careful and will look after all our school ICT equipment by:

□ Not being silly and playing around with it

□ Following our school ICT rules

□ Telling a teacher about anything wrong or damaged.

11. I understand that if I break these rules the school may need to tell my parent(s).

To the parent/caregiver/legal guardian, please:

1. Read this page carefully, to check you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Detach and return this form to the school office
4. Keep the document for future reference, as well as the copy of this signed page which the school will provide.

I understand that Richard Cobden Primary School will:

- Do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment/devices at school, or at school related activities.
- Work progressively with children and their families to encourage and develop an understanding of the importance of online safety through education designed to complement and support the use agreement initiative. This includes providing children with strategies to keep themselves safe on the internet.
- Keep a copy of this signed use agreement on file.
- Respond to any breaches in an appropriate manner.
- Welcome enquiries from parents or students about internet/ICT issues.

My responsibilities include:

- Reading this acceptable use agreement document.
- Discussing the information with my child and explain why it is important.
- Returning the signed agreement to the school.
- Supporting the school's acceptable use programme by encouraging my child to follow the rules, and to always ask the teacher if they are unsure about any use of ICT.
- Contacting the headteacher or school ICT Coordinator to discuss any questions I might have about internet /ICT safety and/or this use agreement and I am welcome to do this at any time.

Please detach and return this section to school.

I have read this acceptable use agreement and I am aware of the school's initiatives to maintain a safe ICT learning environment, including my child's responsibilities.

Name of student: …………………………..……….……….……….………..……….……….……….…....

Name of parent/legal guardian: ……………………….……….……….……….……….……….……….

Parent's signature: ………………………………….…   Date:……………………………...……

Please note: This agreement for your child will remain in force as long as he/she is enrolled at this school. If it becomes necessary to add/amend any information or rule, parents will be advised in writing.

Appendix 2

Pupil iPads Use Guide

Background

Richard Cobden Primary School has **96** iPads available for pupils to use for curriculum purposes. There are **3** trolleys with **32** iPads each on each floor. The trolleys can be found on the corridors.

This policy covers all aspects of the handling and use of these devices. The Staff Acceptable Use Policy and Staff Disciplinary Policy also apply to iPad use at all times and in all locations.

If you wish to use the iPads for your lesson, please write your class name on the borrowing book which can be found on top of the trolleys.

Monitored Use

In common with other school supplied IT systems, staff should have no expectation of privacy when using the iPad. Any and all activity performed on the iPad can be monitored.

All files and photos stored on the iPad should be school related and are subject to reviewing and monitoring.

Use of personal e-mail accounts on pupils' iPads (e.g. Hotmail) and access Social Network sites (such as Facebook, Twitter, Pinterest, etc.) on these devices are not permitted.

Staff and pupils must not:

- Attempt to modify the iPad hardware in any way.
- Apply any stickers or decorations to the iPad.
- Remove the school-supplied case.
- Lend the iPad to others.

Management of iPad Configuration

Pupils' iPads are managed by the school in the same way that the school's laptop and desktop computers currently are.

Staff must not:

- Change any configuration settings on the iPad, particularly network configuration.
- Erase the iPad
- Synchronise the iPad with a computer not belonging to the school
- Change or disable the access password on the iPad.

Staff are responsible for ensuring pupils do not have access to any personal emails, Social networking sites/ apps or photos saved on the iPad.

Damage

If any fault develops, the iPad should be returned to the school's ICT Manager to ensure that the iPad warranty is not compromised.

Lost and Stolen Equipment

If any equipment is lost, the staff member must report it to the school ICT Manager or a member of the Senior Management Team (Headteacher or Deputy Head) immediately. The circumstances of each situation involving lost equipment will be investigated individually.

Online Safety

In order to support the school's Online Safety aims and to verify compliance with the Acceptable Use Policy, Staff iPads will be subject to random spot-checks of browser history and iPad content and configuration. Any inappropriate material or unauthorised configuration changes will be dealt with under the IT discipline process.

Staff should be aware that the location of School iPads is monitored by the use of find my iPad app.

Appendix 3

Acceptable use policy for staff and governors

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (Which is currently: **LGFL**)
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop 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 ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school’s Online Safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Effective From	September 2020
Review Date	September 2023

Richard Cobden School Staff iPad Loan Guide

Background

Richard Cobden School provides an iPad for every staff member to be used for all aspects of teaching and learning and admin purposes.

This policy covers all aspects of the handling and use of these devices. The Staff Acceptable Use Policy and Staff Disciplinary Policy also applies.

General Guidelines

The school's Acceptable Use Policy applies to iPad use at all times and in all locations.

Monitored Use

In common with other school supplied IT systems, staff should have no expectation of privacy when using the iPad. Any and all activity performed on the iPad can be monitored.

All files and photos stored on the iPad should be school related and are subject to reviewing and monitoring.

Ownership and Care

Each iPad remains the property of the school. Staff will have an individually assigned and labelled iPad which will be theirs for the duration of their employment.

Staff should not:

- Attempt to modify the iPad hardware in any way.
- Apply any stickers or decorations to the iPad.
- Remove the school-supplied case.
- Swap iPads with another member of staff
- Dispose of or sell the iPad
- Lend the iPad to others

Management of iPad Configuration

The iPads will be managed by the school in the same way that the school's laptop and desktop computers currently are.

Staff may:

- Sign in and use their own iTunes account on the iPad
- Use iCloud to back up the device
- Add or remove applications from the iPad.
- Use personal email accounts on the iPad (e.g. Hotmail) and access Social Network sites (such as Facebook, Twitter, Pinterest, etc.) but see below for responsibility

Staff may not:

- Change any configuration settings on the iPad, particularly network configuration.
- Erase the iPad
- Synchronise the iPad with a computer not belonging to the school
- Change or disable the access password on the iPad.

Staff are responsible for ensuring pupils do not have access to any personal emails, Social networking sites/ apps or photos saved on the iPad. It is recommended that staff turn off Photo Streaming in the settings to avoid pupils accidentally viewing personal photos.

AUP

The school's Acceptable Use Policy applies to all school-supplied equipment and to all school supplied internet connections.

Staff are reminded that the AUP applies to iPad use in any location – home or school.

Home Use

Staff are allowed to connect their iPad to other WiFi networks but the school cannot provide any technical support in doing this.

Damage

Occasionally, unexpected problems do occur with the iPad that are not the fault of the user. If any faults develop the iPad should be returned to school to ensure that the iPad warranty is not compromised. The iPad warranty will cover normal wear and tear along with any defects that may arise during normal use of the device.

Lost and Stolen Equipment

If any equipment is lost, the staff member must report it to the school immediately.

The circumstances of each situation involving lost equipment will be investigated individually.

Stolen Equipment

Financial Responsibility

Outside of school hours, the iPads are not covered by the school's insurance policy. Any loss or damage will be the responsibility of the staff member. The actual cost of replacement will be determined by Apple but will not exceed the retail value of like-for-like replacement.

Reporting Process

If any equipment is reported as stolen, a police report must be filed and a copy of the report must be provided to the school by the member of staff. If there is not clear evidence of theft, or the equipment has been lost due to negligence, the staff member will be responsible for the full cost of replacing the item(s).

Online Safety

In order to support the school's Online Safety aims and to verify compliance with the Acceptable Use Policy, Staff iPads will be subject to

- random spot-checks of browser history and iPad content and configuration. Any inappropriate material or unauthorised configuration changes will be dealt with under the ICT discipline process.
- Staff are responsible for all content on their iPad including browser history, emails, documents and audio/video content.

Staff should be aware that the location of School iPads is monitored by the use of find my iPad app.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.

I agree to abide by all the points above. I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …………………………………………………… Date……........................

Full Name .... …(printed)

Job title ……………………………………………………………….

Authorised Signature

I approve this user to be set-up.

Signature …………………………………………………… Date……........................

Full Name .... (printed)

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies. I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …………………………………………………… Date……........................

Full Name .... …(printed)

Job title ……………………………………………………………….

Authorised Signature
I approve this user to be set-up.

Signature …………………………………………………… Date……........................

Borrowing ICT Equipment Policy

PURPOSE OF THE POLICY

The purpose of this policy is to set out the policies and procedures in relation to the borrowing of IT equipment by school staff for use in school. No ICT equipment is to be taken off premises without the permission of the ICT Manager.

SCOPE

The policy covers all IT property belonging to the school, the procedures for borrowing, and the responsibilities of the borrower.

DEFINITIONS

'Equipment' refers to all school property, including video and digital cameras, laptops, audio-visual equipment and any other electronic equipment.

POLICY

It is the policy of the school that staff are permitted to use school IT equipment on the understanding that the priority in all cases is that the equipment is available in good condition for the primary purpose of teaching. Staff members wishing to borrow school equipment and/or use school IT equipment off school grounds are required to follow the procedures outlined below:

1. Permission to borrow school equipment must be sought from the IT Coordinator.

2. All equipment to be taken out of school must be 'signed out' by the borrower. The IT Coordinator has the Borrowed Equipment Log. Under no circumstances should any member of staff take home school ICT equipment without written consent of the ICT Manager.

3. Special arrangements must be made with the IT Coordinator for borrowing during the school holidays.

5. All equipment is to be returned and return is acknowledged by signing the 'returned' column of the Log.

6. Damage or loss of property is to be recorded in the sign-out book.

7. By signing out equipment, the borrower accepts the following:

- that occupational health and safety guidelines are followed;

- that where there is any cost to the School of using the equipment or facilities that there be a prior agreed reimbursement; and

- safe use and return of equipment.

- to ensure we uphold our responsibility for data protection, pupil information should not be taken out of school without previous agreement of headteacher. In rare circumstances when this may be necessary, an encrypted storage device must be used. Encrypted USB storage device can be borrowed from the ICT Manager.

Appendix 4

Online Safety incident report form

This form should be kept on file and a copy emailed to Camden's Online Safety officer at jenni.spencer@camden.gov.uk

School/organisation's details

Name of school/organisation: Richard Cobden Primary School

Name of Online Safety contact officer: Alvaro Scrivano
Contact details: 020 7387 5909

Details of incident

Date happened:
Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (cyber bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ online grooming
□ online radicalisation
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

Deliberate access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ cyber bullying □ breach of AUP

Accidental access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

Staff

□ incident reported to head teacher/senior manager
□ advice sought from LADO
□ referral made to LADO
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ Online Safety policy to be reviewed/amended

Please detail any specific action taken (i.e.: removal of equipment)

Child/young person

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ Online Safety policy to be reviewed/amended

Outcome of incident/investigation

Appendix 5 Description of ICT applications

Technology/ Application	**Description/ Usage**	**Benefits**	**Risks**
Internet	Enables the storage, publication and retrieval of a vast range of information Supports communications systems	Provides access to a wide range of educational materials, information and resources to support learning Enables pupils and staff to communicate widely with others Enhances schools management information and business administration systems.	Information is predominantly for an adult audience and may be unsuitable for children The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.
Email	Allows written communications over the network and the ability to attach documents.	Enables exchange of information and ideas and supports collaborative working. Enhances written communications skills A good form of communication for children with some disabilities.	Difficulties controlling contacts and content Use as a platform for bullying and harassment Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems Hacking Unsolicited mail.
Chat/instant messaging	Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people; Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through “buddy lists”.	Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers. Use of pseudonyms protects the child’s identity. Moderated chat rooms can offer some protection to children.	Anonymity means that children are not aware of who they are really talking to. Chat rooms may be used by predatory adults to contact, groom and abuse children on-line. Risk of children giving away personal information that may identify or locate them. May be used as a platform to bully or harass.

Social networking sites	On-line communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging. It allows creation of individual profiles. Users can develop friend's lists to allow access to individual profiles and invite comment.	Allows children to network with peers and join forums to exchange ideas and resources. It provides a creative outlet and improves ICT skills.	Open access means children are at risk of unsuitable contact. Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress. Children may post personal information that allows them to be contacted or located. May be used as a platform to bully or harass.
File sharing (peer-to-peer networking)	Allows users to share computer capability, networks and file storage. Used to share music, video and other materials.	Allows children to network within a community of peers with similar interests and exchange materials.	Illegal download and copyright infringement. Exposure to unsuitable or illegal materials. Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email.	Provide children with a good means of communication and entertainment. They can also keep children safe and allow them to be contacted or stay in contact.	Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. Risk from violent crime due to theft. Risk of cyberbullying via mobile phones.

Effective From	September 2020
Review Date	September 2023