Children, Schools and Families

Online Safety Policy for schools and colleges in Camden

Adapted for The Cavendish School

Reviewed by	Approved by	Updated	Next review
Madeleine Ymeri	ICT Committee	June 2018	Dec 2019

Contents

This Policy applies throughout the School from the EYFS to Year 6.

1 Online Safety: the issues

1.1 Introduction

It is commonly acknowledged that the educational and social benefits for pupils in using the internet should be promoted, but that this should be balanced against the need to safeguard pupils against the inherent risks from internet technology. Further, schools need to be able to teach pupils to keep themselves safe whilst online.

This document provides schools with guidance on developing an effective online safety strategy to enable these aims to be achieved and support staff to recognise the risks and take action to help pupils use the internet safely and responsibly.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, it is imperative that pupils learn computing skills and that the inherent risks are not used to reduce pupils' use of technology. Further, the educational advantages of computing need to be harnessed to enhance pupils' learning.

The table shown at Appendix 4 provides brief details of the various uses of the internet together with their benefits and risks.

The risk associated with use of technology by pupils can be grouped into 4 categories.

1.2.1 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 pupils. There is a danger that pupils may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to pupils, 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 pupils' trust (known as 'grooming') with a view to sexually abusing them.

Pupils 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 pupils at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a pupil, known as online bullying. More details on this can be found in section 4.5 of this Policy.

1.2.3 Commerce

Pupils are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parents' credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade pupils to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Culture

Pupils 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
- Online bullying (see section 4.5 for further details)
- Use of mobile devices to take and distribute inappropriate images of the pupil ('sexting') that cannot be removed from the internet and can be forwarded on to a much wider audience than the pupil intended.

Pupils 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. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable pupils may be at a high degree of risk from such sites. All pupils may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these online.

2 School online safety 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 pupils 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 pupils 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.

In particular, schools must ensure the following:

- A **safe internet platform** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (for example the London Grid
- for Learning (LGfL) platform).
- A culture of **safe practice** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of online behaviour.
- Pupils are **taught to keep themselves and others safe** online and use technology responsibly; this should be achieved by working in partnership with parents and raising awareness of the potential risks of internet use.

2.2 Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole School community, including teaching assistants, Governors and others, and forge links with parents. The strategy must have the backing of the Governors, should be overseen by the Headteacher and be fully implemented by all staff, including technical and non-teaching staff.

2.2.1 Headteacher's role

The Headteacher has 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 to promote online safety and take forward the School's online strategy
- Ensuring online safety is embedded in staff induction and training programmes
- Ensuring online safety is embedded in the curriculum
- Deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

2.2.2 Governors' role

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

Governors should always use School email addresses when conducting School business.

The nominated Governor for online safety matters is Don Kehoe

2.2.3 Online safety co-ordinator'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 co-ordinator should be a member of the Senior Management Team. Given the issues associated with online safety, it is appropriate for the Designated Safeguarding Lead (DSL) to be the School's online safety co-ordinator. This role is jointly undertaken by Isobel Boyt (DSL) and Madeleine Ymeri (Computer Studies 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 that 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 ICT Manager, the Headteacher and nominated Governor to ensure that the School remains up to date with online safety issues and to advise of 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 ICT 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 agreements
- 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

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. Isobel Boyt has been CEOP trained. All staff have undertaken NSPCC online safety training.

2.2.4 ICT Manager's role

Where schools have one, their role is:

- The maintenance and monitoring of the School internet system including anti-virus and filtering systems
- Carrying out monitoring and audits of networks and reporting breaches to the online safety co-ordinator
- Supporting any subsequent investigation into breaches and preserving any evidence.

The School's ICT Manager is Ahmed Abdulkadir

Where schools do not have an ICT manager, support and advice can be provided and the Headteacher or a delegated staff member needs to take responsibility for organising this.

2.2.5 Role of School staff

All School 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 Policy and procedures
- Communicating the School's Online Safety Policy to pupils
- Keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- Planning use of the internet for lessons and researching online materials and resources
- Reporting breaches of internet use to the online safety co-ordinator
- 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 co-ordinator
- Teaching the online safety and digital literacy elements of the curriculum.

2.2.6 Designated Safeguarding Lead

Where any online safety incident has serious implications for the pupil's safety or well-being, the matter should be referred to the School's DSL who will decide whether or not a referral should be made to local authority children's social care or the police. In some schools, the DSL will be the online safety co-ordinator.

The School's DSL is Isobel Boyt; her deputy is Jacqueline Peacock.

2.3 Pupils with special educational needs and disabilities (SEN)

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision.

Learning support co-ordinators are responsible for providing extra support for these

pupils and should:

- Link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEN
- Where necessary, liaise with the online safety co-ordinator and the ICT Manager to discuss any requirements for further safeguards to the School ICT system or tailored resources and materials in order to meet the needs of pupils with SEN
- Ensure that the School's Online Safety Policy is adapted to suit the needs of pupils with SEN
- Liaise with parents and other relevant agencies in developing online safety practices for pupils with SEN
- Keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEN

The School's Learning Support Co-ordinator is Janet Stewart.

2.4 Working with parents

It is essential that schools involve parents in the development and implementation of online safety strategies and policies; most pupils will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at School.

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

The Headteacher, Board of Governors and the online safety co-ordinator 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 should be provided with information on the School's Computer Studies and Acceptable Use Policy and 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.

3 Online safety policies

3.1 Accessing and monitoring the system

- Access to the School internet system should be via individual logins and passwords for staff and pupils wherever possible. Visitors should have permission from the Headteacher or online safety co-ordinator to access the system and be given a separate visitors login
- ICT and technical staff responsible for monitoring systems should be supervised by a member of the Senior Management Team (SMT)
- The online safety co-ordinator and teaching staff should carefully consider the location of internet enabled devices 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 passwords every six months

3.2 Confidentiality and data protection

- The School will ensure that all data held on its ICT systems is held in accordance with data protection law[1]. 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 Bursar immediately. The Bursar will record the security breach and decide whether it warrants reporting to the Information Commissioner's Office
- Where the School uses CCTV, a notice will be displayed in a prominent place to ensure that staff and pupils are aware of this and recordings will not be revealed without appropriate permission

3.3 Acceptable use agreements

- All internet users within the School will be expected to sign an acceptable use agreement annually that sets out their rights and responsibilities and incorporates the School online safety rules regarding their internet use. This will be done each September
- 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 the internet in school (see Appendices 1 and 2). This is done each September
- Staff are expected to sign an acceptable use agreement on appointment. They are expected to be familiar with the School's policies relating to the use of email and social media available via the Employee Handbook and in the Shared Staff folder on the servers.

The School's online safety co-ordinator will keep a copy of all signed acceptable use agreements.

3.4 Teaching online safety

3.4.1 Responsibility

One of the key features of the School's online safety strategy is teaching pupils to protect themselves and behave responsibly while online. 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

[1] General Data Protection Regulation (EU 2016/679), the UK Data Protection Act 2018 and related legislation, The Privacy and Electronic Communications Regulations 2003 and the Protection of Freedoms Act 2012.

applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the Headteacher 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 do so
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum
- 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 PSHCE 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 online
- Teachers should be aware of those pupils who may be more vulnerable to risk from internet use, generally those pupils 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

3.4.2 Content

Pupils should be taught all elements of online safety included in the computing 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

3.5 Staff training and conduct

3.5.1 Training

- All School staff 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/or the ICT Manager
- Staff should also attend specific training on online safety available from CSCB so that they are aware of the risks and actions to take to keep pupils safe online. The SMT should ensure that staff attend regular update training in order to ensure that 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 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. Staff should refer to the School's Social Media Policy 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 educational visits
- Staff should always use School equipment and only store images of pupils taken on or off the School site on the School computer system, never on personal mobile devices
- 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
- Staff should not communicate with pupils directly via email. Pupils should email their work to a secure year group folder
- When making contact with parents by telephone, staff should only use school equipment. Parent numbers should not be stored on a staff member's personal mobile phone and staff should never lend their mobile phones to pupils
- When making contact with parents by email, staff should always use their school email address or account. Personal email addresses and accounts 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 iPads 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 Subject Co-ordinator, Head of Section or Line Manager should liaise with the ICT Manager to ensure that any School equipment is handed over and that PIN numbers, passwords and other access codes are reset so that the staff member can be removed from the School's ICT system.

3.6 Safe use of technology

3.6.1 Internet and search engines

- When using the internet, pupils should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate pupils are the ones who are most at risk
- Primary school pupils 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
- Staff should find and view relevant videos on PCs before allowing access via a large screen. Staff should remain vigilant while material is playing and prepared to close the projection down if anything inappropriate appears
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety co-ordinator, who will liaise with the ICT Manager for temporary access. Teachers should notify the online safety co-ordinator once access is no longer needed to ensure the site is blocked again

3.6.2 Evaluating and using internet content

Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

School email systems should be hosted by an email system that allows content to be filtered and only allows pupils to send emails to others within the School or to approved external email addresses.

Social networking sites such as Facebook, twitter and Instagram 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 online. Some schools may feel that these have an educational value.

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

Gaming-based sites allow pupils to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to pupils. Consequently such sites should not be accessible via school internet systems

Safety rules

- Access to and use of, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses
- If schools identify a clear educational use for emails or social networking sites and forums for online publishing, they should only use sites approved by the ICT Manager. Any use of these sites should be strictly supervised by the responsible teacher
- Emails should only be sent via the School internet system to addresses within the School system or approved external address. All email messages sent by pupils in connection with School business must be checked and cleared by the responsible teacher
- 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 co-ordinator
- Other than those of the DSL and DDSL, individual staff email addresses should not be published on the School website: position emails only should be given e.g. bursar@cavendish-school.co.uk, admissions@cavendish-school.co.uk
- 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
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites
- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, 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, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the School's Anti-bullying Policy for Pupils. This should include any correspondence or contact taking place outside the School and/or using non-School systems or equipment
- Users should be aware that as use of the School internet system is for the purposes of education or school business only, and its use may be monitored
- In order to teach pupils to stay safe online outside of school, they should be advised:
    - Not to give out personal details to anyone online that may help to identify or locate them or anyone else, for example home address, name of School or clubs attended
    - To only use moderated chat rooms that require registration and are specifically for their age group
    - Not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no

control where images may end up or who can see them
    - 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 online and keep communications polite
    - Not to respond to any hurtful or distressing messages but to let their parents know so that appropriate action can be taken
    - Not to give out personal details to anyone online that may help to identify or locate them or anyone else
    - Not to arrange to meet anyone whom they have only met online or go 'off-line' with anyone they meet in a chat room

3.6.4 Video conferencing (where appropriate)

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

- Teachers should try to use a safe video conferencing platform, e.g. LGfL, and need to be aware of the risks associated with live video feeds
- 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 educational visits
- Photographs and videos may only be downloaded onto the School's computer system with the permission of the ICT Manager and should never enable individual pupils' names or other identifying information to be disclosed

3.6.5 School website

- Content should not be uploaded onto the School website unless it has been authorised by the online safety co-ordinator and the Headteacher, 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. This is particularly important where a school allows a number of staff members to upload information onto the website
- To ensure the privacy and security of staff the contact details on the website should be the School address, telephone number and administrative email addresses. Other than the DSL and DDSL, no contact details for staff should be contained on the website
- Pupils' 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

3.6.6 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 pupils are used, prior written consent is obtained from their parents
- Pupils' full names should never be published where their photograph or video is being used
- Staff should ensure that pupils 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 pupil's name
- 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 pupils, 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

3.6.7 Pupils' own mobile phone/handheld systems

- 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
- The use of pupils' personal mobile phones or other devices in classrooms is forbidden. If they are brought to School they must be handed into the School Office on arrival and collected on leaving
- Schools need to be aware that it is considerably more difficult to monitor wireless devices and this should be considered when deciding on the School policy on pupils bringing in and using their own devices. This will also apply to handheld devices such as iPads that are given to pupils by schools for educational purposes
- If schools allow pupils to access their internet system via their own devices, it must be made clear to pupils that the same acceptable use agreements apply and that sanctions may be applied where there is a breach of School policy
- Schools should consider what policy to apply to staff use of their own devices while at School. The School addresses this in its Computer Studies and Acceptable Use Policy

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 co-ordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety co-ordinator on the online safety incident report form (Appendix 3)
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action and consideration given to

contacting the LADO where this is appropriate. Incidents involving the Headteacher should be reported to the Chair of Governors
- The School's online safety co-ordinator 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 DSL, who will make a decision as to whether or not to refer the matter to the police and/or local authority children's social care in conjunction with the Headteacher

Although it is intended that online safety strategies and policies should reduce the risk to pupils whilst online, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. The School cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe online 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 ICT Manager or learning platform provider to ensure that access to the site is blocked and the School's filtering system reviewed to ensure it remains appropriate

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 their acceptable use agreement and subject to appropriate sanctions (see Section 5)
- The incident should be reported to the online safety co-ordinator and details of the website address and URL recorded.
- The online safety co-ordinator should liaise with the ICT Manager or learning platform provider 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 Headteacher and the online safety co-ordinator immediately. If the misconduct involves the Headteacher or a Governor, the matter should be reported to the Chair of Governors
- The online safety co-ordinator will notify the ICT Manager so that the

computer, laptop or other device 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 co-ordinator will arrange with the ICT Manager or learning platform provider 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 Headteacher will take any necessary disciplinary action against the staff member and report the matter to the Governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice
- If the materials viewed are illegal in nature the Headteacher or Governor 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

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. 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.

Online 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 images or videos of someone via mobile phone or email (for example, sexting/happy slapping)

Online 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, online 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 computer studies and acceptable use policies should cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach

- Any incidents of online bullying should be reported to the online safety co-ordinator who will 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 for Pupils. Incidents should be monitored and the information used to inform the development of the School's Anti-bullying Policy for Pupils
- 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 online 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 send or post inappropriate images of themselves
    - 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 pupil as evidence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions. This may be facilitated by the School Council or a specialist resource such as Cybermentors.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing 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. 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. The pupil should also consider changing email address
- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site 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 what measures they can take to block any offensive messages on computers at home

4.5.4 Online bullying of teachers

- Head teachers should be aware that teachers may become victims of online 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 online 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 online bullying involving teachers should be recorded and monitored by the online safety co-ordinator in the same manner as incidents involving pupils
- Teachers should follow the guidance on safe ICT use in section 3.5 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 online bullying of pupils and not reply to messages but report the incident to the Headteacher immediately
- Where the bullying is being carried out by parents, the Headteacher 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 pupils via the internet or mobile devices is a particular issue. Pupils need to know that producing and sharing these images is illegal. Pupils need also 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 by parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of pupils is safeguarded and no young person is unnecessarily criminalized. 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 ICT by older pupils for the purpose of distributing unsuitable materials and sexually harrassing other pupils and be able to safeguard pupils from this.

Online 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 local authority children's social care 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

4.7 Risk from inappropriate contact 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 online.

School staff should also be aware of pupils being sexually abused online through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the online safety co-ordinator and the DSL
- The DSL 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 local authority children's social care/or the police
- The police should always be contacted if there is a concern that the pupil is at immediate risk, for example if they are arranging to meet the adult after school
- The DSL can seek advice on possible courses of action from the online safety officer in local authority children's social care
- Teachers will advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact
- The DSL and the online safety co-ordinator 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 co-ordinator should make a note of all actions taken and contact the ICT Manager or learning platform provider 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 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some pupils may be susceptible to these influences and may be radicalised as a result.

All schools have a duty under the Government's Prevent programme to prevent vulnerable pupils from being radicalised and drawn into terrorism. The main

mechanism for this in Camden is Camden's Channel Panel, a multi-agency forum that identifies pupils who are at risk and develops a support plan to stop the radicalization process and divert them from extremism.

- Staff need to be aware of the School's duty under the Prevent programme and be able to recognize any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against School policies
- The School should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism
- All incidents should be dealt with as a breach of the School's Computer Studies and Acceptable Use Policy, Prevent Policy and Behaviour Policy and staff disciplinary procedures should be used as appropriate
- The online safety co-ordinator and the DSL 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 pupil is being radicalized or is in contact with violent extremists, or that their parents are and this is placing the pupil at risk, schools should refer the young person to the relevant local authority Channel Co-ordinator for support

4.9 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 pupils and desensitise them to the harm. Most pupils who visit these sites will not be adversely affected, but some vulnerable, less resilient pupils may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The School should ensure that pupils have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PSHCE curriculum
- Pastoral support should be made available to all pupils 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 pupils 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 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.

5.1 Sanctions for pupils

Sanctions for pupils will be applied in accordance with the School's Behaviour Policy.

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

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 or prohibited sites during lessons
- Continued unauthorised use of email, mobile phones or social networking sites during lessons
- Use of file sharing software
- Accidentally corrupting or destroying other people's data without notifying staff
- Accidentally accessing offensive material without notifying staff

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems 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
- Online bullying
- Deliberately accessing, sending or distributing offensive or pornographic material
- Purchasing or ordering items over the internet
- Transmission of commercial or advertising material

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 online 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 data protection law
- Bringing the School name into disrepute

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 pupils.

5.2.1 Category A infringements

These are minor breaches of acceptable use policies which amount to misconduct and will be dealt with internally by the Headteacher.

- Excessive use of internet for personal activities not connected to professional development
- Use of personal data storage media (e.g.: removable memory sticks) without carrying out virus checks
- Any behaviour on the world wide web and social media sites such as Facebook, twitter and Instagram 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, including images of pupils or staff, 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 Headteacher who will issue a warning.

5.2.2 Category B infringements

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

- 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 data protection law

- Bringing the School name into disrepute.

Possible sanctions include:

- Referral to the Headteacher
- Removal of equipment
- Referral to the local authority online safety officer
- Referral to the LADO or the police
- Suspension pending investigation
- Disciplinary action in line with School policies

Linked Policies

- Anti-bullying Policy for Pupils
- Behaviour Policy
- Capability and Disciplinary Policy
- Capability and Disciplinary Policy for Employees on Probation
- Code of Conduct for Other Adults in Supervision of Pupils Who Are Not Employees of the School
- Code of Conduct for School Employees
- Computer Studies and Acceptable Use Policy
- Data Protection Policy
- Prevent Policy
- Privacy Notice
- Safeguarding and Child Protection Policy
- Social Media Policy
- Taking, Storing and Using Images of Pupils Policy
- Whistleblowing Policy

APPENDIX 1

THE CAVENDISH SCHOOL

Key Stage 1: Computer Studies Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to in school and at home	
2. I **CHECK** before I use new sites, games or apps with a trusted adult	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say they are	
6. I don't keep **SECRETS** just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared, just not sure or if I have made a mistake	

My trusted adults are:

_____ at School and

_____ at home

My name is _____

Parent signature _____

APPENDIX 2

THE CAVENDISH SCHOOL

Key Stage 2: Computer Studies Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the School's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to. If I make a mistake I know that I can tell a trusted adult.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.

- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Pupil signature _____ Date _____

Parent signature _____ Date _____

APPENDIX 3

ONLINE SAFETY INCIDENT REPORT FORM (CAMDEN TEMPLATE)

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

School details:

Name of school _____

Address _____

Name of online safety co-ordinator _____

Contact details _____

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 setting ☐ Outside school setting

Who was involved in the incident?

☐ Pupil ☐ Staff member ☐ Other (please specify)

Type of incident:

☐ Bullying or harassment (online bullying)

☐ Deliberately bypassing security or access

☐ Hacking or virus propagation

☐ Racist, sexist, homophobic religious hate material

☐ Terrorist material

☐ Drug/bomb making material

☐ Child abuse images

☐ Online 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	☐ Online 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 Headteacher/SMT

☐ Advice sought from Children's Safeguarding and Social Work

☐ Referral made to Children's Safeguarding and Social Work

☐ Incident reported to police

☐ Incident reported to social networking site

☐ Incident reported to ICT Manager

☐ Disciplinary action to be taken

☐ Online Safety Policy to be reviewed/amended

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

_____

_____

☐ **Pupil**

☐ Incident reported to Headteacher/SMT

☐ Advice sought from Children's Safeguarding Services and Social Work

☐ Referral made to Children's Safeguarding Services and Social Work

☐ Incident reported to police

☐ Incident reported to social networking site

☐ Incident reported to ICT Manager

☐ Pupil's parents informed

☐ Disciplinary action to be taken

☐ Pupil debriefed

☐ Online Safety Policy to be reviewed/amended

Outcome of incident/investigation

_____

_____

_____

Appendix 4: Description of online 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 pupils • 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 pupils 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/ gaming	• Chat rooms allow users to chat online in real time in virtual meeting places with a number of people • Instant messaging allows real- time chat for 2 or more people privately with no-one else able to join. Users have control over who they contact through 'buddy lists'	• Enhances social development by allowing pupils to exchange experiences and ideas and form friendships with peers • Use of pseudonyms protects the pupil's identity • Moderated chat rooms can offer some protection to pupils	• Anonymity means that pupils are not aware of who they are really talking to • Chat rooms may be used by predatory adults to contact, groom and abuse pupils on- line • Risk of pupils giving away personal information that may identify or locate them • May be used as a platform to bully or harass

Social networking sites	• Online 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 friends lists to allow access to individual profiles and invite comment	• Allows pupils to network with peers and join forums to exchange ideas and resources • It provides a creative outlet and improves computer studies skills	• Open access means pupils are at risk of unsuitable contact • Risk of pupils posting unsuitable material online that may be manipulated to cause them embarrassment or distress • Pupils 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 pupils 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 pupils with a good means of communication and entertainment • They can also keep pupils 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 online bullying via mobile phones