
# CCfL E-safety Policy Final

| | |
|---|---|
| Name of policy | CCfL E-safety Policy |
| Date reviewed | Spring 2017 |
| Staff member Responsible | Jeanette Lowe |
| Governor Responsible | Tony Burgess |
| Date signed off by Governors | Spring 2017 |

**CCfL: KS3 School: 020 7974 3953. CCfL KS4 School: 020 7974 8906**

**Challenge Yourself, Celebrate Achievement, Focus on Success, Learn for Life**

# Contents

# 1 Information on internet technology

## 1.1 Introduction

It is commonly acknowledged that the educational and social benefits for student in using the internet should be promoted, but that this should be balanced against the need to ***safeguard*** student against the inherent risks from internet technology. Further, CCfL need to be able to teach students to keep themselves safe whilst on-line.

This document provides CCfL with guidance on developing an effective e-safety strategy to enable these aims to be achieved and support staff to recognise the risks and take action to help student 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. The table shown at ***Appendix 5*** provides brief details of the various uses of the internet together with their benefits and risks.

As use of technology is now universal, it is imperative that student learn computing skills in order to prepare them for the working environment; and that the inherent risks are not used to reduce student's use of technology. Further, the educational advantages of computing need to be harnessed to enhance student's learning.

The risk associated with use of technology by student 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 student. There is a danger that student 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 student as users can take on an alias rather than their real names and can hide their identity. Adults, who pose as students, in order to befriend and gain student's trust ("***known as "grooming***") with a view to sexually abusing them, may use the sites.

Student 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 student 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).

### 1.2.3 Commerce

Students 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 parent's 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 student to reveal computer passwords or other information about the family for the purposes of fraud.

### 1.2.4 Culture

Student 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)

- use of mobile devices to take and distribute inappropriate images of the young person (**sexting**) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Student 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 student may be at a high degree of risk from such sites. All students may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

# 2 CCfL e-safety strategies

## 2.1 Purpose and description

Computing is now a key part of the CCfL curriculum and one of the key aims of computing is to ensure that students are aware of e-safety messages. This is part of the CCfL responsibility to safeguard and promote the welfare of students, as well as the duty **of care to student** and their parents to provide a safe learning environment.

CCfL should have an e-safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe e-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 student from harm
- safeguard staff in their contact with students and their own use of the internet
- ensure the CCfL fulfils its duty of care for students
- provide clear expectations for staff and students on acceptable use of the internet.

In particular, CCfL 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 platform).

- A culture of ***safe practice*** underpinned by a strong framework of e-safety policy that ensures everyone is aware of expected standards of on-line behaviour.

- Students are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

## 2.2 Roles and responsibilities

***A successful e-safety strategy needs to be inclusive of the whole CCfL community, including teaching assistants, supervisory assistants, governors and others, and forge links with parents and carers.*** The strategy must have the backing of CCfL governors, should be overseen by the head teacher and be fully implemented by all staff, including technical and non-teaching staff.

### 2.2.1 Head teacher's role

*Head teachers have ultimate responsibility for e-safety issues within the CCfL including:*

- *the overall development and implementation of the CCfL's e-safety policy*
- *ensuring that e-safety issues are given a high profile within the CCfL community*
- *linking with the board of governors and parents and carers to promote e-safety and forward the CCfL's e-safety strategy*
- *ensuring e-safety is embedded in the curriculum*
- *deciding on sanctions against staff and students who are in breach of acceptable use policies.*

### 2.2.2 Governors' role

***Governing bodies*** have a ***statutory responsibility*** for student safety and should therefore be aware of ***e-safety*** issues, providing support to the head teacher in the development of the CCfL's e-safety strategy.

Governors should be subject to the same e-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 CCfL business.

### 2.2.3 E-safety contact officer's role

The CCfL should have a designated e-safety contact officer who is responsible for co-ordinating e-safety policies on behalf of the CCfL. Ideally, the contact officer should be a senior member of the management team. Given the issues associated with e-safety, ***it is appropriate for the designated child protection teacher to be the CCfL's e-safety contact officer***.

*The e-safety contact officer should have the authority, knowledge and experience to carry out the following:*

- ***develop, implement, monitor and review the CCfL's e-safety policy***
- ***ensure that staff and students are aware that any e-safety incident should be reported to them***
- ***provide the first point of contact and advice for CCfL staff, governors, students and parents***
- ***liaise with the CCfL's computing manager/co-ordinator to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher***

- ***assess the impact and risk of emerging technology and the CCfL's response to this in association with IT staff and learning platform providers***
- ***raise the profile of e-safety awareness with the CCfL by ensuring access to training and relevant e-safety literature***
- ***ensure that all staff and students have read and signed the acceptable use policy (AUP)***
- ***report annually to the board of governors on the implementation of the CCfL's e-safety strategy***
- ***maintain a log of internet related incidents and co-ordinate any investigation into breaches***
- ***report all incidents and issues to Camden's e-safety officer.***

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

### 2.2.4 IT manager's role

Where CCfL have one, their role is:

- *the maintenance and monitoring of the CCfL internet system including anti-virus and filtering systems*
- *carrying out monitoring and audits of networks and reporting breaches to the e-safety contact officer*
- *supporting any subsequent investigation into breaches and preserving any evidence.*

Where CCfL do not have an ***IT manager***, support and advice can be provided and the head teacher or a delegated staff member needs to take responsibility for organising this.

### 2.2.5 Role of CCfL staff

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

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

- ***teaching the e-safety and digital literacy elements of the new curriculum.***

### 2.2.6 Designated child protection teachers

*Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection teacher for the CCfL who will decide whether or not a referral should be made to Family Services and Social Work or the Police.* At the CCfL, the designated child protection teacher will be the e-safety contact officer, who will liaise with the Curriculum lead for ICT and the ICT and data manager re appropriate polices, systems and guidance.

## 2.3 Students with special needs

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

*SEND co-ordinators are responsible for providing extra support for these students and should:*

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

## 2.4 Working with parents and carers

It is essential that CCfL involve parents and carers in the development and implementation of e-safety strategies and policies; most students 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 CCfL.

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

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

***Parents should be provided with information on computing and the CCfL's e-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 CCfL as well as the CCfL's expectations regarding their behaviour.***

# 3 E-safety policies

## 3.1 Accessing and monitoring the system

- *Access to the CCfL internet system should be via individual log-ins and passwords for staff and students wherever possible. Visitors should have permission from the head teacher or e-safety contact officer to access the system and given a separate visitor's login.*

- *The e-safety contact officer should keep a record of all log-ins used within the CCfL for the purposes of monitoring and auditing internet activity.*

- *A senior member of their management team should supervise network and technical staff responsible for monitoring systems.*

- *The e-safety contact officer 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 students depending on their age and experience.*

## 3.2 Acceptable use policies

- *All internet users within the CCfL will be expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the CCfL e-safety rules regarding their internet use.*

- *Students and their parents should both sign the acceptable use policy, and use of the internet at the CCfL is dependent on signing this agreement* ***(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 2).***

*The e-safety contact officer will keep a copy of all signed acceptable use agreements.*

## 3.3 Teaching e-safety

### 3.3.1 Responsibility

*One of the key features of the CCfL's e-safety strategy is teaching students to protect themselves and behave responsibly while on-line. There is an expectation that over time, students 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 e-safety education lies with the head teacher and the e-safety contact officer, but all staff should play a role in delivering e-safety messages.*

- *The e-safety contact officer is responsible for ensuring that all staff has the knowledge and resources to enable them to do so.*

- *Teachers are primarily responsible for delivering an ongoing e-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 students of expectations on internet use and the need to follow basic principles in order to keep safe.*

- *Teachers may wish to use PSHE/ICT lessons as a forum for discussion on e-safety issues. To ensure that students understand the risks and why it is important to regulate their behaviour whilst on-line*

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

- *Teachers should ensure that the CCfL's policy on students' use of their own mobile phones and other mobile devices in CCfL is adhered to.*

### 3.3.2 Content

*Students should be taught all elements of e-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.*

### 3.3.3 Technology and sexual abuse and bullying behaviour

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

For example, sexting involves the sending of intimate photographic images of an individual to others electronically via the internet. Students 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.

***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, CCfL need to include responses to sexual bullying in their behaviour policy and make a referral to Family Services and Social Work for any student who displays sexually abusive behaviour towards other students. Staff should refer to Camden's "Student who harm other student" guidance for further details on this.

## 3.4 IT and safe teaching practice

*CCfL 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 students. Staff should refer to the model social media policy for CCfL staff for further guidance.*

*Staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations should follow the following points.*

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

- *Staff should always use CCfL equipment and only store images on the CCfL 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 students 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 CCfL or specific students 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 students via instant messaging or social networking sites as these may be misinterpreted or taken out of context.*

- *Where staff need to communicate with students regarding CCfL work, this should be via the CCfL 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 students by telephone, staff should only use CCfL equipment. Student or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to students.*

- *When making contact with parents or students by email, staff should always use their CCfL email address or account. Personal email addresses and accounts social media accounts should never be used.*

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

- *Where staff is using mobile equipment such as laptops or i-pads provided by the CCfL, they should ensure that the equipment is kept safe and secure at all times.*

## 3.5 Safe use of technology

### 3.5.1 Internet and search engines

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

- *CCfL Nurture student should be supervised at all times when using the internet. Although supervision of CCfL older students will be more flexible, teachers should remain vigilant at all times during lessons.*

- *Students 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 students to in-advertently 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 e-safety contact officer, who will liaise with the IT service provider for temporary access. Teachers should notify the e-safety contact officer once access is no longer needed to ensure the site is blocked.*

### 3.5.2 Evaluating and using internet content

*Teachers should teach students 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.*

### 3.5.3 Safe use of applications

***CCfL email systems*** *should be hosted by an email system that allows content to be filtered and allow students to send emails to others within the CCfL or to approve email addresses externally.*

***Social networking sites*** *such as Facebook, MySpace and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have been blocked by the CCfL but students are likely to use these sites at home.*

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

***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, students will use these at home although CCfL internet systems do host these applications.*

***Gaming-based sites*** *allow student 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 student. Consequently, such sites should* ***not be accessible*** *via CCfL internet systems*

***Safety rules***

- *Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the CCfL internet system* ***is forbidden*** *and* ***blocked****. This is to protect students from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.*

- *If CCfL identify a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.*

- *Emails should only be sent via the CCfL internet system to addresses within the CCfL system or approved external address. All email messages sent by students in connection with CCfL 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 e-safety contact officer who will liaise with the learning platform provider.*

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

- *Students 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.*

- *Students 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 student receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.*

- *Students 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 CCfL's anti-bullying policy. This*

*should include any correspondence or contact taking place outside the CCfL and/or using non-CCfL systems or equipment.*

- *Users should be aware that as users of the CCfL internet system is for the purposes of education or CCfL business only, and its use may be monitored.*

- *In order to teach students to stay safe online outside of CCfL, 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, school name 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 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.*
    - *not to give out personal details to anyone on-line that may help to identify or locate them or anyone else*
    - *not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room*
    - *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.*

### 3.5.4 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, ie: London Grid for Learning and need to be aware of the risks associated with live video feeds.*

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

- *Teachers should ensure that students 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 CCfL trips.*

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

### 3.5.5 CCfL website

- *Content should not be uploaded onto the CCfL website unless it has been authorised by the e-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.*

- *CCfL should designate a named person or persons to have responsibility for uploading materials onto the website. This is particularly important where a CCfL allows a number of staff members to upload information onto the website.*

- *To ensure the privacy and security of staff and students, the contact details on the website should be the CCfL address, email and telephone number. No contact details for staff or students should be contained on the website.*

- *Student'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 CCfL and the intended audience.*

### 3.5.6 Photographic and video images

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

- *Where photographs or videos of student 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.*

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

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

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

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

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

- *CCfLs should inform parents that although they may take photographic images of CCfL events that include other student, 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.*

### 3.5.7 Students own mobile phone/handheld systems

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

However, many parents prefer their student to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. Generally, use of personal mobile phones or other devices should be forbidden in classrooms.

CCfL need to be aware that it is considerably more difficult to monitor wireless devices and this should be considered when deciding on the CCfL policy around *students* bringing in and using their own devices. This will also apply to handheld devices such as i-pads that are given to *students* by CCfL for education purposes.

If CCfL will allow *students* to access the CCfL internet system via their own devices, it must be made clear to *students* that the same acceptable use agreements apply and that sanctions may be applied where there is a breach of CCfL policy.

CCfL should record their policy here:

| |
|---|
| Students at Key Stage 3 are allowed to bring phones and mobile devises into school but they must be handed in at the office where they are stored securely until the student leaves at the end of the day.<br><br>Students at Key Stage 4 may be allowed to keep their mobile phones on them as long as they do not use them in lessons or use them inappropriately. |

They should not take images of staff for other students and if they do they will be asked to leave their phones at home and /or their parents will be called in. If they take and use any images further sanctions will be applied including involvement of the school safer school officer and police action.
Please see use of mobile phones agreement.

Students cannot access the CCfL Internet system.

# 4 Responding to incidents

## 4.1 Policy statement

- All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety contact officer in the first instance. The e-safety contact officer on the e-safety incident report form (appendix 3), whether involving students or staff, must record all incidents.

- A copy of the incident record should be emailed to Camden's designated e-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 and consideration given to contacting the LADO where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors.

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

- E-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 Family Services and Social Work in conjunction with the head teacher.

Although it is intended that e-safety strategies and polices should reduce the risk to *students* whilst on-line, this cannot completely rule out the possibility that *students* may access unsuitable material on the internet. Neither the CCfL 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 student or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately (and calmly) close or minimise the screen.*

- *Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the CCfL's "no blame" approach.*

- *The incident should be reported to the e-safety contact officer and details of the website address and URL provided.*

- *The e-safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the CCfL's filtering system reviewed to ensure it remains appropriate.*

## 4.3 Intentional access of inappropriate websites by students

- *If a student 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 e-safety contact officer and details of the website address and URL recorded.*

- *The e-safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.*

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

## 4.4 Inappropriate use of IT by staff

- *If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the e-safety contact officer immediately. If the misconduct involves the head teacher or governor, the matter should be reported to the chair of the board of governors.*

- *The e-safety contact officer will notify the network 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 e-safety incident report form.*

- *The e-safety contact officer will arrange with the network 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 head teacher will take any necessary disciplinary action against the staff member and report the matter to the CCfL 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 head teacher or governor should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.*

## 4.5 Cyberbullying

### 4.5.1 Definition and description

Cyberbullying 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 CCfL 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 *students* 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").

Cyber bullying can affect students 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 students at the CCfL, whether or not they take place on CCfL premises or outside CCfL.

- *CCfL 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 e-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 CCfL'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 e-safety awareness and education, students should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.*

- *Students 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 young person as evidence.*

Any action taken on cyber bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the *students* involved to resolve the issues themselves rather than impose sanctions. This may be facilitated by the CCfL staff or a specialist resource such as Cyber mentors.

### 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 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 students 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 student should also consider changing email address.*

- *Where bullying takes place in chat rooms or gaming sites, the student 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 on what measures they can take to block any offensive messages on computers at home.*

### 4.5.4 Cyberbullying of teachers

- *Head teachers should be aware that teachers may become victims of cyberbullying by students. 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 students.*

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

- *Incidents of cyber bullying involving teachers should be recorded and monitored by the e-safety contact officer in the same manner as incidents involving students.*

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

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

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

## 4.6 Risk from inappropriate contacts and non-contact sexual abuse

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

CCfL staff should also be aware of *students* being sexually abused on-line 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. The perpetrators may be adults but may also be peers.

- *All concerns around inappropriate contacts should be reported to the e-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 students involved, before deciding whether or not to make a referral to Family Services and Social Work 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 CCfL.*

- *The designated child protection teacher can seek advice on possible courses of action from Camden's e-safety officer in Family Services and Social Work.*

- *Teachers will advise the student how to terminate the contact and change contact details where necessary to ensure no further contact.*

- *The designated child protection teacher and the e-safety contact officer should always notify the student'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 CCfL IT equipment or networks, the e-safety contact officer should make a note of all actions taken and contact the network 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 students is minimised.*

## 4.7 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 young people may be susceptible to these influences.***

- *Staff need to be aware of those students who are being targeted by or exposed to harmful influences from violent extremists via the internet. Students and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against CCfL policies.*

- *The CCfL should ensure that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism.*

- *All incidents should be dealt with as a breach of the acceptable use policies and the CCfL's behaviour and staff disciplinary procedures should be used as appropriate.*

- *The e-safety contact officer and the designated child protection teacher should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the CCfL and whether current CCfL procedures are robust enough to deal with the issue.*

- *If there is evidence that the students is becoming deeply enmeshed in the extremist narrative, CCfL should seek advice from* ***Camden's Integrated Youth Support Services*** *on accessing programmes that prevent radicalisation. Where there is evidence that their parents are involved in advocating extremist violence, referral should be made to FSSW.*

## 4.8 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 CCfL 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 CCfL IT

The CCfL is 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 that CCfL may want to adopt: For each point, CCfL may record their own detailed list of breaches and corresponding sanctions.

## 5.1 Sanctions for students

### 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 e-safety contact officer.*

**CCfL policy**
**Sanctions would be implemented in line with the school's Behaviour Policy**
**This would include tutor action and consequences**

### 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 e-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.*

*Sanctions could include:*

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

**CCfL policy**
**Sanctions would be implemented in line with the School's Behaviour Policy**
**This would include parents being contacted and agreed sanctions being implemented**

### 5.1.3 Category C infringements

*These are deliberate actions that either negatively affects CCfL 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*
- *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 e-safety contact officer*
- *referral to head teacher*
- *loss of access to the internet for a period of time*
- *contact with parents*
- *any sanctions agreed under other CCfL policies.*

**CCfL policy**
**Sanctions would be implemented in line with the school's Behaviour Policy**
**This would include parents being called in for a meeting and agreed sanctions being implemented.**

### 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 CCfL 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 e-safety officer.*

**CCfL policy**
**Sanctions would be implemented in line with the school's Behaviour Policy**
**This would include involvement of the Safer school officer and/or police action.**

## 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 student.*

### 5.2.1 Category A infringements

*These are minor breaches of the CCfL'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 (e.g.: removable memory sticks) without carrying out virus checks*
- *any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the CCfL and community, for example inappropriate comments about*

*the CCfL, staff or students 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.*

| **CCfL policy**<br><br>**This would include referral to the Head teacher and possibly the school disciplinary process being followed** |
|---|

### 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 student. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO.*

- *serious misuse of or deliberate damage to any CCfL 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 CCfL name into disrepute.*

*Possible sanctions include:*
- *referral to the head teacher*
- *removal of equipment*
- *referral to Camden's e-safety officer*
- *referral to Camden's LADO or the police*
- *suspension pending investigation*
- *disciplinary action in line with CCfL policies.*

| **CCfL policy**<br><br>**This would include referral to the Head teacher and the school disciplinary process being followed** |
|---|

Appendix 1:

***Acceptable use policy for CCfL Students***

***Name:***
***CCfL:***
***Class:***

*I understand that the CCfL owns all computer equipment and that I can use the internet at CCfL as long as I behave in a responsible way that keeps me and others safe. I also understand that the CCfL ICT system is monitored and that if I do not follow the rules, I may not be allowed to use the CCfL computers.*

*I will:*

- *only use the CCfL's computers for CCfL work and homework*
- *only delete my own files and not look at other people's files without their permission*
- *keep my login and password safe and not let anyone else use it or use other people's login or password*
- *not bring in files to CCfL without permission*
- *ask a member of staff for permission before using the internet*
- *not visit websites I know are banned by the CCfL or use non-CCfL email accounts or social networking sites*
- *only email people I know or whom my teacher has approved*
- *make sure any messages I send or information I upload is polite and sensible*
- *not open attachments or download files unless I have permission or I know and trust the person who sent it*
- *not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends unless my teacher has given permission*
- *never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me*
- *tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like and I will not respond to any bullying messages*
- *only use my mobile phone or other device in CCfL when I have permission*
- *not use any internet system to send anonymous or bullying messages or to forward chain letters*
- *log out when I have finished using the computer.*

*Signed:*
*Date:*

***Parents***

□ *I have read the above CCfL rules for responsible internet use and agree that my child may have access to the internet at CCfL. I understand that the CCfL will take all reasonable precautions to ensure students do not have access to inappropriate websites, and that the CCfL cannot be held responsible if students do access inappropriate websites.*

□ *I agree that my child's work can be published on the CCfL website.*

□ *I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.*

*Signed:*
*Date:*

Appendix 2

## *Acceptable use policy for staff and governors*

### *Access and professional use*

- *All computer networks and systems belong to the CCfL and are made available to staff and governors for educational, professional, administrative and governance purposes only.*

- *Staff and governors are expected to abide by all CCfL e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or governors being removed.*

- *The CCfL reserves the right to monitor internet activity, examine, and delete files from the CCfL's system.*

- *Staff and governors have a responsibility to safeguard students in their use of the internet and reporting all e-safety concerns to the e-safety contact officer.*

- *Copyright and intellectual property rights in relation to materials used from the internet must be respected.*

- *E-mails and other written communications must be carefully written and polite in tone and nature.*

- *Anonymous messages and the forwarding of chain letters are not permitted.*

- *Staff and governors will have access to the internet as agreed by the CCfL but will take care not to allow students to use their logon to search the internet.*

### *Data protection and system security*

- *Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the CCfL premises via laptops and other mobile systems, the information must be encrypted beforehand.*

- *Use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented on the CCfL ICT system using SOPHOS software.*

- *Downloading executable files or unapproved system utilities will not be allowed and all files held on the CCfL ICT system will be regularly checked.*

- *Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.*

- *Files should be saved, stored and deleted in line with the CCfL policy.*

***Personal use***

- *Staff and governors should not browse, download or send material that could be considered offensive to colleagues and students or is illegal.*

- *Staff and governors should not allow CCfL equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.*

- *Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the CCfL's name into disrepute.*

- *CCfL ICT systems may not be used for private purposes without permission from the head teacher.*

- *Use of CCfL ICT systems for financial gain, gambling, political purposes or advertising is not permitted.*

*I have read the above policy and agree to abide by its terms*

***Name:***

***CCfL:***

***Signed:***

***Date:***

Appendix 3:

**E-safety incident report form**
*This form should be kept on file and a copy emailed to Camden's e-safety officer at jenni.spencer@camden.gov.uk*

**CCfL details:**

**Name of CCfL:**

**Address:**

**Name of e-safety contact officer:**

**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 CCfL/service setting □ Outside CCfL/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
□ 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 Family Services and Social Work
□ referral made to Family Services and Social Work
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended

**Please detail any specific action taken (ie: removal of equipment)**

□ **Child/young person**

□ incident reported to head teacher/senior manager
□ advice sought from Family Services and Social Work
□ referral made to Family Services and Social Work
□ 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
□ e-safety policy to be reviewed/amended

## Outcome of incident/investigation

## Appendix 4: Description of ICT applications risk assessment

| Technology/ Application | Description/ Usage | Benefits | Risks |
|---|---|---|---|
| Internet | • Enables the storage, publication and retrieval of a vast range of information<br>• Supports communications systems | • Provides access to a wide range of educational materials, information and resources to support learning<br>• Enables students and staff to communicate widely with others<br>• Enhances, the CCfL management of information and business administration systems | • Information is predominantly for an adult audience and may be unsuitable for student<br>• The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information<br>• 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.<br>• Enhances written communications skills<br>• A good form of communication for student with some disabilities | • Difficulties controlling contacts and content<br>• Use as a platform for bullying and harassment<br>• Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems<br>• Hacking<br>• Unsolicited mail |
| Chat/instant messaging/ gaming | • Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people;<br>• 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 | • Enhances social development by allowing student to exchange experiences and ideas and form friendships with peers.<br>• Use of pseudonyms protects the child's identity.<br>• Moderated chat rooms can offer some protection to student. | • Anonymity means that student are not aware of who they are really talking to.<br>• Chat rooms may be used by predatory adults to contact, groom and abuse student on-line<br>• Risk of student giving away personal information that may |

| | | | |
|---|---|---|---|
| | "buddy lists". | | identify or locate them<br>• 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<br>• It allows creation of individual profiles.<br>• Users can develop friend's lists to allow access to individual profiles and invite comment. | • Allows student to network with peers and join forums to exchange ideas and resources.<br>• It provides a creative outlet and improves ICT skills. | • Open access means student are at risk of unsuitable contact.<br>• Risk of student posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress<br>• Student may post personal information that allows them to be contacted or located.<br>• 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.<br>• Used to share music, video and other materials | • Allows student to network within a community of peers with similar interests and exchange materials | • Illegal download and copyright infringement<br>• Exposure to unsuitable or illegal materials<br>• 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 student with a good means of communication and entertainment.<br>• They can also keep student 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.<br>• Risk from violent crime due to theft<br>• Risk of cyber bullying via mobile phones. |