fortismere

Digital Technology Policy

Introduction for stakeholders

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

At Fortismere we understand the responsibility to educate our students on Digital Safety issues. Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

A shared responsibility
Everybody in our school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Breaches
A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure

This policy is in two parts:

1. Staff Guidelines and Responsibilities which is also included in Staff Safeguarding Policy
2. Parents/ Carers/Students Guidelines and Responsibilities, which is given and signed by all parents at the start of their child’s school career.

Part 1 Staff Guidelines and Responsibilities

Roles and Responsibilities

The Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors, parents, carers and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy, Confidentiality and Schools Safe.

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff keep all school-related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work- based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.
  The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff must inform Leadership if they receive an offensive e-mail
- However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Receiving e-Mails

- Check e-mail regularly
- Activate 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult the network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-mailing Personal, Sensitive, Confidential or Classified Information

Where staff's conclusion is that e-mail must be used to transmit such data:

- Obtain express consent from line manager to provide the information by e-mail

- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details have not been separately verified (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt
- Use own school e-mail account so staff member is clearly identified.
- Always check that confidential information is relevant to named party

Skills Development for Staff

- Staff receives regular information and training on eSafety and how they can promote the 'Stay Safe' online messages.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Incident Reporting, e Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to School Management.

Misuse and Infringements

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to senior management team/Head of department/Head of Faculty/ head of College
- Deliberate access to inappropriate materials by any user will lead to an investigation by the Headteacher/ LA and could possibly lead to dismissal and involvement of police for very serious offences.

Managing the Internet

- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

Internet Use

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Staff must not reveal names of colleagues, pupils, others or any other confidential information acquired through their role on any social networking site or other online application
- On-line gambling or gaming is not allowed

Infrastucture

- Staff are aware that school based email and internet activity can be monitored and explored further if required
- If staff discovers an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of staff
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the School Office.

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from own PC or removable media equipment is kept secure
- Staff must ensure that screen is locked before moving away from the computer during the normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Only download personal data from systems if expressly authorised to do so by team leader
- Staff must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Staff to keep screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Remote Access

- Staff are responsible for all activity via remote access facility
- Only use equipment with an appropriate level of security for remote access
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought and a copy is located in the personnel file

Portable & Mobile ICT Equipment

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by our ICT support

Social Media, including Facebook and Twitter

- Staff are advised not to access their personal social media accounts at any time during school hours on school equipment.
- Staff are advised to make all social media sites secure so that they remain confidential to users selected network group

- Staff and governors are aware that their online behaviour should at all times be compatible with UK law

Telephone Services

- School telephones are provided specifically for school business purposes.

Summary

Review Procedure
There will be on-going opportunities for staff to discuss with Leadership.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

Further help and support these websites are helpful:
http://www.saferinternet.org.uk/advice-and-resources/young-people/11-19s
http://www.commonsensemedia.org/
https://www.facebook.com/safety
Advice on esafety - http://www.thegrid.org.uk/eservices/safety/policies.shtml
Test our online safety skills [http://www.getsafeonline.org]

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for our own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.   Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
For more information Department for Education.

Part 2: Student and Parent Guidelines and Responsibilities

E Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e Safety guidance to be given to students on a regular and meaningful basis. E safety is embedded within our curriculum and we continually look for new opportunities to promote E Safety. Colleges actively promote through assemblies and VT activities on ways to keep safe and to understand the harm misuse can cause to others.

- The school has a framework for teaching internet skills.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating students about the online risks that they may encounter outside school is also done informally when opportunities arise and as part of the E Safety curriculum
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/ carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research
- Students using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems

e-Mails

- All student and parent e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a parent/ carer /teacher/ trusted adult if they receive an offensive e-mail.

Safe Use of Images

Taking of Images and Film

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Head teacher/SLT images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Head teacher/SLT
- Students and staff must have permission from the Head teacher/SLT before any image can be uploaded for publication

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.
Student's full names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Student's full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the School Office web manager or the Head teacher has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network

Personal Mobile Devices (including phones)

- Students are allowed to bring personal mobile devices/phones to school but must not use them within lesson time.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Managing Other Web 2 Technologies
It is the parents/ carers responsibility to ensure that they work within the law in relation to web 2 technologies AND THAT AGE LIMITS ARE ADHERED TO.

- Students are not permitted to access their social media accounts on school equipment whilst at school
- All students are advised to be cautious about the information given by others on social networking websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests)
- Students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Students are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Headteacher

Incident Reporting, Misuse Inappropriate Material

- Students are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to a member of staff.

- Deliberate access to inappropriate materials by any student will lead to an investigation by the Head teacher/ LA and could possibly lead to a permanent exclusion and involvement of police for very serious offences.

Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement or similar
  - We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - School website
  - Newsletter items

Guidelines to support you when talking to your child about digital technologies

1. Boundaries: There are age limits on certain technologies, make sure that you are aware.
2. Adjust settings on parental controls in line with your child's age and maturity.
3. Social networking sites: make yourself a friend so you can monitor activities. Remind your child that anything posted can be seen, copied, changed and forwarded to other people. Prospective employers also look .
4. Talk to them about information found and how it might be detrimental, how they can protect their privacy.
5. Discuss how they behave to others and what they post online and inappropriate sites.
6. Discuss downloading and plagiarism- so they are aware of the legal implications.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

Concerned about your child's safety online?

Kidsmart.org.uk Provides easy to use advice on how to keep your child safe. Kidsmart is provided by Childnet.

Us Online 2 - New ways to understand our online world.

Insafe – is a European network of Awareness Centres promoting safe, responsible use of the internet and mobile devices

UKCCIS - The UK Council for Child Internet Safety (UKCCIS) brings together organisations from industry, charities and the public sector to work with the government to deliver the recommendations from Dr Tanya Byron's report

Childline - Childline is a free 24 hour counselling service for children and young people up to 18 in the UK

ChildLine 0800 1111

Bullying UK - Bullying UK is a UK charity founded in 1999 by Journalist Liz Carnell and her son John. The charity's website provides a large amount of information to help pupils, parents and schools deal with bullying.

http://www.saferinternet.org.uk/advice-and-resources/young-people/11-19s

Acts Relating to eSafety

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for our own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Student Acceptable Use – (Guidelines) Sample

Agreement / Digital Technologies Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- **I will only use my school e-mail address.**
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Head teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others’ work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Dear Parents and Carers

Digital Technology Safety at Fortismere School

I am writing to ask for our support in ensuring that students are aware of how to stay safe when using the internet. At school we teach our students how to stay safe on-line and how to behave appropriately on-line. In order to develop a home-school partnership on on-line safety, I would like you to discuss the attached 'Acceptable Use Agreement' and sign it with your child. If you have any concerns or queries, please do not hesitate to get in touch.

Please fill in and return the bottom section of this form by:

Many thanks once again

Kind regards

Helen Anthony
Headteacher

Pupil and Parent/Carer signature……………………………………………………………………………..

We have discussed this document and ……………………………………..........(student name) agrees to follow the Digital rules and to support the safe and responsible use of ICT at Fortismere School

Parent/ Carer Signature …………………….………………………………

Pupil Signature……………………………………………………………….

Form ………………………………… Date ………………………………

SAFER INTERNET DAY 2014

Let's create a better internet together

SAFER INTERNET DAY 2014
TUESDAY 11 FEBRUARY
Let's create a better internet together
www.saferinternetday.org

Conversation starters for parents and carers

Ask your children to tell you what they like most about the internet and why e.g. sites they visit, ways to communicate, games they play etc.

What does a better internet mean to them?
(Is it safer, kinder, more fun, with more to do, fewer age restrictions etc?)

Ask your children what they would like others to do, to improve or change the internet and make it a better place.

What could your children do themselves to make the internet a better place? Do they have creative skills, or ideas, to design a great new website or app?

Ask them to tell you how they stay safe online. What tips do they have for you, to deal with online issues, and where did they learn them?

Ask your children if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.

Encourage your children to help others. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.

Think about how you each use the internet. What more could you do to use the internet together? Are there activities you could enjoy as a family?

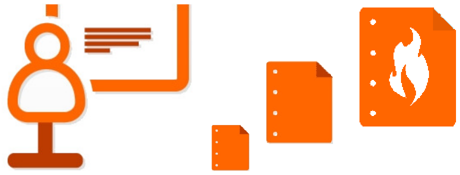
Co-funded by the European Union

For more information please visit:
www.saferinternet.org.uk

UK Safer Internet Centre
www.saferinternet.org.uk

INFORMATION & ONLINE RESOURCES

1. CHILDNET RESOURCES AND WEBSITES

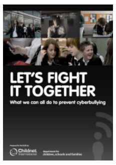


Childnet: Childnet International is a non-profit organisation working in partnership with others around the world to help make the internet a great and safe place for children. The Childnet website hosts all the online resources detailed below, as well as a number of recommended resources for young people, parents, carers and teachers. **www.childnet.com**

Childnet resources: On our website you can access resources on a range of topics, including our previously branded Know IT All for Parents interactive guide. The **Parents and Carers** area also contains key advice, information on reporting and detailed information on a range of e-safety topics in the **Hot topics** section. **www.childnet.com/parents-and-carers**

UK Safer Internet Centre: Childnet is part of the European Commission appointed UK Safer Internet Centre. Together with partners the Internet Watch Foundation and the South West Grid for Learning, we raise awareness about internet safety, develop information materials and resources and organise high profile events such as Safer Internet Day. You can access a range of resources from across the UK, Europe and wider afield at **www.saferinternet.org.uk**.

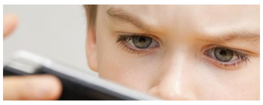
Digizen: A website providing information and advice to encourage responsible digital citizenship. It shares advice and guidance on preventing and responding to cyberbullying, including the film '**Let's Fight It Together**' and specific information on social networking. **www.digizen.org**



KidSMART: This award winning Childnet website is for children, teachers, parents and carers and offers fun games and activities for children alongside effective internet safety advice. Don't forget to check out our new Early Surfers' Zone for 3-7 year olds where you can read the online stories '**The Adventures of Smartie the Penguin**' and '**Digiduck's Big Decision**.' **www.kidsmart.org.uk**

2. PARENTAL CONTROLS & FILTERING

A Parents' Guide to Technology: The UK Safer Internet Centre has created this guide to answer commonly asked questions and introduce some of the most popular devices used by children, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly. **www.saferinternet.org.uk/parent-tech**



Childnet's guide to **Online Gaming** also contains helpful advice and information. **www.childnet.com/ufiles/Online-gaming.pdf**

Internet Parental Controls: The four big internet providers - BT, Sky, Talk Talk and Virgin Media - provide their customers with free parental controls that can be activated at any time. Video tutorials on how to download and use these controls are available on the UK Safer Internet Centre website. **www.saferinternet.org.uk/parental-controls**

3. COMPUTER PROTECTION & SECURITY

Sorted: This website was produced by young people and looks at the issues of internet security and protection. It gives simple explanations, important information and advice on how to protect a computer from the dangers of programmes such as viruses, phishing scams, spyware and trojans. **www.childnet.com/sorted/**

Get Safe Online: A government website which focuses on online computer security and protection issues. It contains advice about firewalls, spyware and antivirus protection as well as how to protect children online. **www.getsafeonline.org**

4. SOCIAL NETWORKING

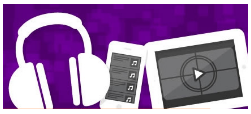
Young People & Social Networking Sites: Aims to help parents understand the positive and creative ways young people are using social networking spaces (eg Facebook, Twitter and Google+). It also points out the potential risks of using these sites and ways to minimise these risks.
www.childnet.com/ufiles/Young-people-and-social-networking-A.pdf

Facebook Family Safety Centre: Provides useful information and tips for parents and carers, teens and educators. These pages do not require a Facebook account in order to view them. **www.facebook.com/safety**

Google+ Safety Centre: Provides useful information and tips for parents and carers, teens and educators. These pages do not require a Google account in order to view them.
www.google.com/+/safety

Twitter Help Centre - Tips for Parents: Provides useful information and tips for parents and carers. These pages do not require a Twitter account in order to view them.
support.twitter.com

5. FILE SHARING & DOWNLOADING



Music, Film, TV and the Internet: Childnet has developed this guide with the music, film and television industries to inform parents, teachers and young people about how to stay safe and legal when enjoying entertainment on the internet or via a mobile device.
www.childnet.com/resources/downloading

The Content Map: A UK based website that signposts to legal online retailers of film, TV, music, games, ebooks and sports coverage. **www.thecontentmap.com**

6. SEARCH ENGINES

Using a child friendly search engine allows content to be filtered. Most adult search engines, such as Google, Bing and YouTube, also have built in filtering options under the 'preferences' link that should be adjusted before use.

Google Family Safety Centre: **www.google.co.uk/goodtoknow/familysafety**

BBC: **www.bbc.co.uk/cbbc/find**

Yahoo!: **kids.yahoo.com**

Ask Kids: **www.askkids.com**

7. WHERE TO REPORT

Need help? Information about what to do if a child comes to you for help and advice about how to report online concerns such as cyberbullying, inappropriate content or illegal behaviour.
www.childnet.com/parents-and-carers/need-help

Child Exploitation and Online Protection (CEOP): A police agency tackling child abuse on the internet. This website includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online. **www.ceop.police.uk**
CEOP's **Think U Know** website contains information for children and parents, as well as a link for children to report abuse online. **www.thinkuknow.co.uk**

Internet Watch Foundation: The UK's hotline for reporting illegal content found on the internet. It deals specifically with child abuse and criminally obscene images hosted in the UK and internationally. **www.iwf.org.uk**

ParentPort: A website run by the UK's media regulators, allowing you to report content unsuitable for children found in a programme, advert, film, video game, newspaper/magazine or other forms of media. **www.parentport.org.uk**

Find us on Facebook: **childnetinternational**

Follow us: **@childnet**

Subscribe to our newsletter to stay up to date: **www.childnet.com**