King
Ecgbert
School

E-safety Policy

Date ratified:	5.12.2012
Governors/Committee Meeting:	Curriculum and Personnel
Signature of Chair:	*Chris Newman*

Contents

Overview

This e-safety policy was created through consultation with a number of stakeholders in King Ecgbert School consisting of:

Emma Anderson (Child Protection Liaison Team Leader and Deputy Head)
David Willis (E-Safety Co-ordinator and Deputy Head teacher)
Jackie Arundale (Deputy CPLT and Deputy Head)
Caroline Wheelhouse (ICT Head of Department and E-Safety Co-ordinator for learning)
Francesca Hutton (Office Manager)

Any questions, queries or concerns relating to this policy or any e-safety issues in general should be discussed with a member of the **e-safety Management Group** which consists of **the staff named above.**

The policy was completed on: 16 November 2012.

The policy was approved by the governing body of King Ecgbert School on 21 November 2012.

This policy is due for review no later than 16 November 2013.

Introduction

King Ecgbert School recognises the immense benefits that ICT, internet, MLE and a wide range of electronic communication provide for the development of high quality learning experiences across our school community.

We wish to actively promote engagement in the range of technologies available throughout our whole school community. With the advent of student and parental engagement through our MLE, a whole new level of communication and active engagement is available to us which enables us to operate within a wholly transparent and cohesive learning environment.

King Ecgbert School also recognises the need to balance the benefits of these technologies with a thorough awareness of the potential risks. It is vital that our whole school community understands and adheres to the e-safety policy that ensures safe, appropriate and responsible use of such technologies. This policy is designed to reflect our commitment to the safeguarding and well being of our students.

Responsibilities of the King Ecgbert School Community

We believe that e-safety is the responsibility of the whole school community and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the e-safety Management Group

The e-safety log will be reviewed every half term by the CPLT and the Safeguarding Governor. Any necessary action will be taken.
Promote an awareness and commitment to e-safety throughout the school.
Be the first point of contact in school on all e-safety matters.
Lead the school e-safety group.
Create and maintain e-safety policies and procedures.
Develop an understanding of current e-safety issues, guidance and appropriate legislation.
Ensure all members of staff receive an appropriate level of training in e-safety issues
Ensure that e-safety education is embedded across the curriculum.
Ensure that e-safety is promoted to parents and carers.
Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
Monitor and report on e-safety issues to the e-safety group and SLT as appropriate
Ensure an e-safety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

Read, understand and help promote the school's e-safety policies and guidance.
Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
Develop and maintain an awareness of current e-safety issues and guidance.
Model safe and responsible behaviours in your own use of technology.
Embed e-safety messages in learning activities where appropriate.
Supervise students carefully when engaged in learning activities involving technology.
Be aware of what to do if an e-safety incident occurs.
Maintain a professional level of conduct in their personal use of technology at all times.
Breaches of e-safety will be dealt with in line with staff and student codes of conduct.

Please note that any visitors to school who may be shadowing or supporting a department must only access the school network under supervision of a member of staff.

Responsibilities of Technical Staff and staff with specific roles linked to ICT

Read, understand, contribute to and help promote the school's e-safety policies and guidance.
Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
Support the school in providing a safe technical infrastructure to support learning and teaching.
Report any e-safety related issues that come to your attention to a member of the e-safety Management Group.
Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to your work.
Liaise with the local authority and others on technical issues.
Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Students

Read, understand and adhere to the school student Acceptable Use Policy (AUP).
Help and support the school in creating e-safety policies and practices and adhere to any policies and practices the school creates.
Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know someone who this is happening to. Discuss e-safety issues with family, friends and staff in an open and honest way.

Responsibilities of Parents and Carers

Read, understand and promote the school student AUP with your children.
Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

Read, understand, contribute to and help promote the school's e-safety policies and guidance.
Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
Ensure appropriate funding and resources are available for the school to implement their e-safety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.

We will provide a series of specific e-safety related lessons in every year group as part of the ICT, L@kes and PSHCE curriculum.

We will celebrate and promote e-safety through planned assemblies.

We will discuss, remind or raise relevant e-safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

We will remind students about their responsibilities through an end-user AUP which every student will sign. The student AUP will be displayed throughout the school and displayed when a student logs on.
Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- include useful links and advice on e-safety on our school website, parent site of the MLE and through our school newsletter.

- Consult parents through parental survey

Managing ICT Systems and Access

King Ecgbert School, in partnership with Civica, will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

Servers, workstations and other hardware and software will be kept updated as appropriate.

Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.

The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

All users will sign an end-user Acceptable Use Policy (AUP) provided by the school. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.

All King Ecgbert students will access the Internet using an individual log-on, which they will keep secure.

Whether supervised by a member of staff or working independently, students will abide by the school AUP at all times.

Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.

The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.

The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

Filtering Internet access

The school uses a filtered Internet service. The filtering is provided through YHGFL. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform a member of the e-safety Management Group.

If users discover a website with potentially illegal content, this should be reported immediately to a member of the e-safety Management Group. The school will report this to appropriate agencies including the filtering provider.

The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

Our policy on staff and student use of a range of learning technologies is summarised in the following table. Staff and students should also refer to the Acceptable Use Policy whenever engaging with such technologies.

	Students	Staff
Personal mobile phones brought into school	Mobile phones must be switched off and out of sight during the school day.	Staff allowed
Mobile phones used in lessons	Students allowed with permission as part of a learning activity	Staff not allowed unless exceptional permission given by member of SLT
Taking photographs or videos on personal equipment	Students allowed with permission as part of a learning activity	Staff will use school equipment for taking photos and videos where possible. Images taken using personal equipment must be for educational purposes only and deleted immediately after storage, in a secure area of the school network.
Taking photographs or videos on school devices	Students allowed with permission as part of a learning activity	Staff allowed as part of a school based activity providing data is not taken off site
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Students allowed with permission as part of a learning activity or during designated break times but not for recreational use during lessons e.g. listening to music.	Staff allowed during designated breaks
Use of personal email addresses in school	Students not allowed	Staff allowed but not for school business
Use of school email address for personal correspondence	Students allowed	Staff allowed
Use of online chat rooms	Students not allowed	Staff not allowed
Use of instant messaging services	Students not allowed	Staff allowed during designated breaks
Use of blogs, wikis, podcasts or social networking sites	Students allowed with permission as part of a learning activity	Staff allowed as part of a school based activity

Using email

Staff and students should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.

Students will be allocated an individual e-mail account for their use in school.

Students will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.

Communication between staff and students or members of the wider school community should be professional and related to school matters only.

Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

We will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Digital images, video and sound will only be created in school using equipment provided by the school or on personal equipment under the supervision of a member of staff.

Staff and students will follow the school policy on creating, using and storing digital resources. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/students involved.

If students are involved, relevant parental permission will also be sought before resources are published online.

Parents are entitled to opt out of their child having photographs, videos or other images taken.

Using blogs, wikis, podcasts, social networking and other ways for students to publish content online

Within school, blogging, podcasting and other publishing of online content by students will only take place within the school learning platform. Students will not be allowed to post or create content on sites where members of the public have access. Any exceptions to this rule would need to be authorised by the e-safety group.

Students will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them. Students will not use their real name when creating such resources. They will be encouraged to create an appropriate ‘pseudonym’.

Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using mobile phones

Personal mobile phones will only be used during lessons with permission from the teacher. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone should be provided and used. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a student or parent.

Using new technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-safety point of view.

We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-safety risk.

Protecting Personal Data

We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff will ensure they properly log-off from a computer terminal after accessing personal data.

Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure. Data taken off site should be encrypted via a portable device such as a USB.

Staff must ensure that their access to Sims takes place in a secure environment and should never leave Sims open if unattended. Staff should be particularly vigilant if Sims is open during a lesson and ensure that students are not able to access sensitive data. No SIMS data including registers or personal data/information will ever be displayed on the IAW

When downloading or transferring data to the MLE department site or specific class site staff must ensure such data is not transferred to the student site of the MLE where students would have access to potentially sensitive data.

The school website and other online content published by the school

The school website will not include the personal details, including individual e-mail addresses or full names, of staff or students.

A generic contact e-mail address will be used for all enquiries received through the school website.

All content included on the school website will be approved by a member of the e-safety Management Group before publication.

The content of the website will be composed in such a way that individual students cannot be clearly identified.

Staff and students should not post school-related content on any external website without seeking permission first.

Dealing with e-safety incidents

It is vital that all members of our school community are fully aware of the potential incidents that may arise from improper use of technologies, the importance of being constantly vigilant in the monitoring and reporting of any such incidents and that improper and inappropriate use of technologies will result in a staged approach to sanctions including the removal of internet permissions for a fixed period of time, in addition to the full range of other behaviour sanctions in line with the School behaviour Policy. Staff are reminded that improper and inappropriate use of technologies in school may result in disciplinary or criminal action depending on the severity of the offence.

Potential breaches of protocol which must be avoided

Students and staff

- Accessing illegal content deliberately
- Accessing inappropriate content deliberately
- Accessing illegal content accidentally and failing to report this
- Accessing inappropriate content accidentally and failing to report this
- Inappropriate use of personal technologies (e.g. mobile phones) at school
- Accessing social networking sites, chat sites, instant messaging accounts or personal emails where not allowed
- Accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
- Downloading or uploading files where not allowed
- Sharing your username and password with others
- Accessing school ICT systems with someone else’s username and password
- Opening, altering, deleting or otherwise accessing files or data belonging to someone else
- Using school or personal equipment to send a message or create content that is offensive or bullying in nature
- Attempting to circumvent school filtering, monitoring or other security systems
- Sending messages or creating content that could bring the school in to disrepute
- Revealing the personal information (including digital images, video or text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- Use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

Staff only

- Transferring personal data insecurely
- Using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones or communicating via social networking sites)
- Failure to abide by copyright of licensing agreements (for instance, using online resources in lessons where permission is not given)

King Ecgbert School - Student Acceptable Use Policy

Acceptable Use of ICT for Students at King Ecgbert School

The school allows you to use the computers and other devices in school to access the Internet to help you with your learning. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment.

- You will only use the ICT systems and other devices for school work and homework. You should seek permission first for any other use.
- You should keep usernames and passwords safe and do not reveal these to anyone else. Only log on using your own account.
- You should not deliberately search for, view, download, upload or forward material that is illegal or that would be considered offensive by another user. This includes content that is pornographic, racist or violent in nature.
- If you encounter any content or communications that is unpleasant or upsetting, or you believe is illegal or would be considered offensive by another user, you should report this to a member of staff immediately.
- Only send messages to people you know, using your school email address or other school-created accounts. Other contacts should be agreed with a member of staff before messages are sent.
- Any messages you send, content you post online or work you create using the school ICT systems must be polite and responsible. It is not acceptable to harass, offend or cause upset to any other user. This includes taking or creating digital photos or videos of other staff or pupils without their consent.
- Any messages you send or posts you make to websites, in or out of school-time, should not cause staff, pupils or other users distress or bring the school into disrepute.
- You should not give away any of your personal information, or the personal information of other users in school, over the Internet. This includes photographs or video images of yourself, other pupils or members of staff.
- You will not arrange to meet someone you only know online unless this is part of schoolwork, in which case you will inform a member of staff and should ask a responsible adult, parent or guardian to go with you.
- You should respect intellectual property and ownership of online resources you use in your schoolwork, and ensure you acknowledge all sources you use.
- You should not attempt to change any settings or install any software on equipment without permission. You should ask permission from a member of staff before downloading files or resources from the Internet.
- You should not attempt to bypass any security, filtering or monitoring systems that may be active on equipment. They are there for your protection and safety. If you feel a legitimate resource is being accidentally blocked you should ask a member of staff to investigate for you.
- You should check any files brought in on removable media, such as USB sticks or CDs, to ensure they are free of viruses and other malware before use. Files brought in from home should only be directly related to school work.
- You should not connect any personal equipment such as mobile phones, cameras or media players to the school ICT system, or attempt to access the school network from any personal equipment, unless this is part of an educational activity and you have permission from a member of staff.
- You should not attempt to access or delete resources, files or messages belonging to someone else.
- You should not waste valuable time and resources on activities that are not directly related to school work.
- The school will ensure you receive regular eSafety information and guidance, and you will take an active responsibility in assessing the potential risks of the technology you use, and for using such technology (in and out of school) in a safe, responsible and legal way.

I have read and understood the above statements and I agree to comply with King Ecgbert School rules for use of ICT facilities and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Student signature…………………………………………………………………Form Group…………….

Student full name………………………………………………………………Date………………………

King Ecgbert School – Staff Acceptable Use Policy

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes as agreed by the school senior management team
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
- You should not attempt to download or install any hardware or software. All requests should be through the Civica help desk
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems e.g. learning platforms. It is not acceptable to contact pupils using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of pupils and staff should be for professional purposes only. They should be taken on school equipment, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.

- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school eSafety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching

Finally:
You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.

Finally:
You understand that your files, communications and Internet activity will be monitored and checked at all times. If these statements or other guidance from the school are not followed, action may be taken to protect yourself or others, including restricting your access to the school ICT systems. In certain circumstances it may be necessary to confiscate personal equipment to protect yourself and other users

I have read and understood the above statements and I agree to comply with King Ecgbert School rules for use of ICT facilities and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Staff member's signature..
Staff member's full name..

Date..

Appendix A

Child Internet Safety

Did You Know?

12% of children have experienced data misuse such as identity theft or somebody using their personal information in a way they didn't like - **EU Kids Online II**

13% of 12-15 year olds are happy to share their email with 'friends of friends' or 'anyone'. Children are happier to share photos and feelings online compared to sharing personal contact details - **Ofcom**

Around 25% of 8-15 year olds with a social networking profile have it set to open, either to anyone or to friends and their friends - **Ofcom**

41% of 12-15 year olds have a smartphone and around half use it for social networking on a weekly basis - **Ofcom**

29% of children in the UK have had online contact with people they had not met before - **EU Kids Online II**

12% of 8-11 year olds and 24% of 12-15 year olds say that they use social networking sites to communicate with people not directly known to them – **Ofcom**

The Child Exploitation and Online
Protection Centre (CEOP) receives more than 600 reports of grooming a month

11% of children in the UK have encountered sexual images online and 12% of 11-16 year olds have received them - **EU Kids Online II**

21% of UK children say they have been bullied and 8% say this occurred on the internet - **EU Kids Online II**

19% of UK 11-16 year old internet users have seen one or more type of potentially harmful user-generated content, rising to 32% of 14-16 year old girls - **EU Kids Online II**

45% of 12-15 year olds claim to understand how search engines operate but one third say they think all search engine information is truthful - **Ofcom**

Introduction

For young people, the internet and the increasing number of digital devices they use to connect to it, is an integral part of their everyday lives. Whether they use it to express themselves or to stay in touch with friends, for entertainment or education, the internet can provide tremendous benefits and most use it safely. But while digital technology provides a wealth of opportunities, we are all aware that there are online risks and sometimes these risks can lead to harm. At the same time, while young people's 'offline' and 'online' worlds are often merging, the behaviours and safeguards of the 'real' world are not always applied in the virtual world where friends can be added at the click of a button and information shared in an instant.

EU Kids Online is a research project which surveyed 25,000 children and their parents across Europe to understand the true online risks and opportunities. It defines the risks young people might be exposed to online under three key headings:

Content
Harm that can arise from exposure to age inappropriate, distasteful or illegal content.

Conduct
Harm that can arise from how young people behave online

Contact
Harm that can arise from interactions with other individuals online

A fourth category 'Commerce' is also sometimes added. This reflects the concerns that some have about the exposure of children to messages of a sexual and commercial nature.

Although many children are taught some aspects of internet safety in school, we can play an important part in helping to safeguard young people online. By offering **clear, prominent and accessible** advice and by integrating this advice throughout the school, particularly at the **point of provision**, we can help ensure that children and young people can safely get the most from the services we offer and can direct them to.

48% of children in the UK say that there are things on the internet that bother children their own age and 13% of 9-16 year olds say that they've been bothered/upset by something online (EU Kids Online)

Around 10% of 8-15 year olds who use the internet at home report seeing things that make them feel sad, frightened or embarrassed online (Ofcom)

What is chatting?

There are lots of different ways you can chat to people online – and lots of different places you can do it. Chatting includes every type of service which allows you to have a conversation with somebody else. It can be text based messaging (such as instant messaging or SMS) or via a voice or video link (such as by VoIP internet phone calls or a webcam). It can also be instant, real time communication (chat rooms or instant messaging) or delayed (such as e-mail or voicemail). Chatting like this is a great way to get in touch – as well as meet new people. But there are a few things you can do to make sure that you have a good time and stay safe.

Things to think about

Know who you are talking to online; if you don't know someone face to face they could be anyone

Remember – what you do or show on your webcam can be recorded and what they do or show on their webcam at the other end might be a recording

Avoid having one-sided webcam conversations where the other person's webcam is 'broken' or 'not working...'; you won't know who they really are, what they are doing or who they are watching with

Things to do

Keep your personal information private – avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust

Check whether the service you use allows you to create friends lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information

Keep your clothes on when using webcam – images of you could end up in the wrong hands

Use private messages for people you know in person and trust; be careful of private messaging people you don't know

Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, change it). An example would be 1%43?Owl765HP.

Know how to block someone if they make you feel uncomfortable or upset

Learn how to save chat logs and texts so that if someone does make you uncomfortable/upset, you have the evidence to report them

Remember to log out of a service properly after use, especially on a shared computer.

Additional advice for parents/carers

Talk to your child about who they're talking to online and encourage them to think before talking to people they don't know in person

Try to understand and guide your child's online behaviour – negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends'.

Familiarise yourself with the chat programme your child uses. Find out more about built in safety functions and how they can be contacted within the service

Ask your child if they know how to block someone who they don't want to talk to anymore. If they don't, help them learn how to use the blocking feature

Use parental control software provided by your internet service provider, mobile phone network, online content provider or games console and consider using filtering options, monitoring and setting time limits for access to chat

If you discover misconduct between your child and someone online stay calm, investigate the facts and seek expert help if needed.

As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality, which may include sexual chatting

Reporting

If someone makes you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.

If someone is bullying you, there is help and support available from CyberMentors

If the problem concerns issues of privacy, or a breach of terms of service, report the issue to a teacher in school.

CLICK CEOP Internet Safety

Sharing

What is sharing?

If you have something you're proud of then it can feel good to share it with others. Maybe its a photo you've taken or a video you've made. Maybe you have opinions and thoughts you want to share on a forum or in your own blog, or you want to share your interests with people who like the same things as you. One of the great things about sharing on the internet is that it's so quick and easy – you just click a button on your computer, smartphone or digital camera and it's there online. But that can also be the problem. If you post something in haste you may regret it later and by that time it may be too late to get it back. Here are some things you should think about before you ever share things online.

Things to think about

- Once you’ve shared something online you’ve lost control and ownership of it
- Remember that people may still be able to see things that you share online months or even years into the future
- If you’re unsure about what you should and shouldn’t share online, ask yourself this: “Would I show this to my parents/carers/teachers?’ If you wouldn’t, then don’t share it online
- Some people could use information or things you’ve shared in ways you don’t like or couldn’t have imagined
- Some people could share things about you which are upsetting – without your knowledge

Things to do

- Find out how to use the privacy settings on the service you use. These settings will help you take control of your information so that you can decide what information you will share and who you will share it with
- Keep your personal information private – this includes photos of you and your friends, your school name, email, phone number, date of birth, address and location; only share them with people you know and trust
- Only upload pictures of yourself which you would be happy for your parents/carers or teachers to see
- Only share details of your location with people you know in person and trust

Additional advice for parents/carers

- Set up a family email address you can all use to fill in online forms
- Set clear guidelines for your children about what is ok to share about themselves and about your family – lead by example and explain what you have shared and why; be aware that comments posted by your children could impact on you and your family’s reputation
- Talk to your children about how easy it is for people to assume another identity online
- There are a number of ways that you can set your own lists of sites you want to block access to; activating your internet service provider’s parental controls, or those of another provider, can make this easy for you
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date
- Be aware that children can access the internet through publicly available wifi for example in shops, coffee bars and bus termini; check whether your

children's devices have built in wifi connectivity and see if there are any tools to help manage access to inappropriate content

- As part of a wider discussion about sex and relationships, cover how people may use the internet to explore their sexuality which may include sharing sexual images
- Be aware that smartphones often contain location technology. This technology finds the mobile's position and provides services related to where you are. Talk to your child about who they share this information with

Reporting

- Know/learn what to do if you have shared something that you shouldn't have
- If someone has shared information about you which upsets you, or if someone is making you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline on 0800 1111. If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you using your information, there is help and support available from CyberMentors and BeatBullying.
- Know what to do if something online has upset you: talk to Childline or the Samaritans if you are feeling desperate or sad, B-eat for eating disorder advice and go to Report-it to report incidents of race hate.

Gaming

What is gaming?

Playing games online against other people can be really enjoyable and great fun. You can do it via a mobile phone, a computer or a games console and games come in every shape and form. There are the ones where you each take a turn – like chess on a mobile phone app – and others where you compete to get your scores as high as you can on a leaderboard. Then there are the 3D virtual worlds where hundreds of thousands of people are simultaneously playing against each other. Online gaming has something for everyone and millions of children and young people across the UK regularly taking part. Below are some tips to ensure you get the most out of your online gaming experience.

Things to think about

- When you're gaming as part of a network this often involves live online chat and you're playing with real people.
- You should be respectful to others in the game and understand the rules and boundaries of the website or community.

Things to do

- Keep gaming friends ‘in the game’ – avoid sharing personal information with people you’ve met in games and avoid giving them your social networking profile details or email address. Also, choose a user name that does not reveal any personal information about you.
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you’ve ever shared your password in the past, change it). An example would be 1%43?Owl765HP.
- Learn how to block people you don’t want to be in contact with anymore. If you experience any bullying, hacking and racism, save the evidence and report it.
- Remember to always log out of a service properly after use, especially on a shared computer.
- Experts recommend you take regular 5 minute breaks every 45 minutes to an hour to help your concentration.

Additional advice for parents/carers

- Young people can also go online through some gaming devices and online gaming often involves playing against real people.
- Use the PEGI games ratings to guide you when buying games for your child or making judgements about the games they are playing. The PEGI system rates video games at various age levels (3,7,12,16 and 18) and is designed to protect children and young teenagers from inappropriate content.
- Make sure your children are using games from reputable and legal online providers
- Online gaming can be compulsive for some; be aware of the amount of time spent online and set boundaries around your child’s use.
- Games should be played as part of a healthy and balanced lifestyle; regular 5 minute breaks should therefore be taken every 45 minutes to an hour.
- Use parental controls on games consoles to disable or restrict access to facilities such as voice chat. They can also be used to disable online credit payments or applications that you feel are inappropriate.
- You can use parental online controls to restrict or block access to online gaming websites and other content altogether.
- Familiarise yourself with the chat programme your child uses. Find out more about its built in safety functions.

- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date

Reporting

- Know where to get help if someone is bullying you in a game – us as a school or talk to CyberMentors and BeatBullying who can provide help and support
- If someone is upsetting you or making you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline on 0800 1111. If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.

CLICK CEOP Internet Safety

Content providing (including downloading)

What is content providing?

There is so much information available on the internet that it's like having the world's biggest library available at your fingertips. But not everything that you read and see online will be true, and not everyone will be who they say they are. It is also illegal to download some files, while others could be infected with viruses which steal your personal details and pass them on to thieves. Below are a few things you need to consider when browsing the web – and a few steps you can take to keep yourself safe:

Things to think about

- Not everything you see or read online is true – it is easy for people to make things up or alter photos on the internet
- There are things online you might find upsetting or distressing – you will know what these things are
- Downloading may harm your computer or mobile device and may be illegal – just because you can download something, it doesn't mean that you are allowed to or should do, as copyright law applies online. This is especially true of illegal file sharing sites
- If you make music, film or TV available to others on a file sharing network, down load from an illegal site or sell copies without the permission of those who own the copyright then you are breaking the law; use legal sites that reward the creators for their work

- Copying someone else’s ideas and passing them off as your own is called plagiarism – our school has rules about this.

Things to do

- Learn how to block pop ups
- Check whether information is true by looking on at least two other sites; ignore sites you don’t recognise and consider carefully what you are reading
- Use reputable sources of information such as organisations or brands you know and trust
- Only download files from websites you are sure are safe to use; sites might contain malicious software (such as viruses) which could damage your computer or steal your personal information.
- Only open attachments or click on links in emails you are expecting; if you get a suspicious looking email, even from a friend, it might not be genuine if their computer has been infected by a virus and you should not open it.
- Think – if an offer seems too good to be true, it probably is.

Additional advice for parents/carers

- Set safe search filters and lock this on for a particular desktop computer, laptop or mobile
- Use parental controls to manage access; mobile operators use network filters which block ‘Over 18’ content; these are free of charge and are mostly set as ‘on’ by default by all contract and prepay customers.
- Use software filters on computers, laptops and mobile; most fixed internet service providers offer these free to customers
- Around one in every 100/200 emails can contain malware (a piece of malicious software which takes over a person’s computer) or phishing attacks (attempts to access your personal details such as usernames and passwords): install reputable antivirus or firewall software on your computer or mobile and make sure you keep this and operating systems up to date
- As part of a wider discussion about sex and relationships, cover how people may use the internet to explore their sexuality, which may include viewing pornography

Reporting

- If you come across something which upsets you, you can talk to an adult that you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). You can talk to Childline or The Samaritans if you feel sad or desperate, B-eat for eating disorder support and Report-it to report incidents of race hate.

- Illegal child sex abuse images online can be reported to the Internet Watch Foundation (IWF) or your local police.
- You can report fraud or online scams or viruses to Action Fraud – the UK's national fraud reporting centre.
- Get Safe Online provides advice on how people can use the internet confidently, safely and securely.

Networking (closely relates to 'sharing')

What is networking?

Online communities – such as social networking sites – are some of the most popular sites on the web. Millions of people log onto these sites every day to hang out with their friends and talk about their lives. When you sign up you get the chance to create and customise your own profile and you can upload your favourite photos and videos. There are even networks within networks where you can join others who share the same interests, or who live in the same area or go to this school. Most people will have a great time being a member of these sites – but it's important you take care, particularly when giving out information about yourself. Here are some tips on how to network safely.

Things to think about

- Adding someone as a friend means they (and sometimes their friends) may be able to see the things you share, share things with you and even shre things about you; can you trust them with your information?
- It's easy to lie online, not everyone is who they say they are

Things to do

- Learn about privacy settings to take control of your information and decide what information you will share, and who you will share it with – use lists/groups to share different information with different 'friends'
- Avoid friending people you don't know in person and sharing personal information with them such as your phone number, home address or photographs
- Learn how to block 'friends' in case you feel you need to, and keep the evidence
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, change it). An example would be 1%43?Owl765HP.

- Think very carefully about meeting someone face to face who you only know online; if you do decide to do this, never go without taking a trusted adult with you
- Only upload or share pictures of yourself which you would be happy for your parents/carers or teachers to see.
- Remember to properly log out of a site after use, especially on a shared computer.

Additional advice for parents and carers

- Keep an open dialogue with your child about who they are talking to online and why they should think before talking to people they don't know in person; try to understand and guide their online behaviour just as you would for their offline activity; negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends' (and 'friends of friends').
- Use parental controls to restrict or block access to social networking sites; device-level parental controls mean that you can set up unique settings per user so that you can restrict access to particular networks based on the user.
- Explain why it's important to be honest about your age online, for example in signing up to social networking sites – advertising and other content will be aimed at the age the user says they are.
- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality

Reporting

- If someone is making you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you using your information, there is help and support available from CyberMentors and BeatBullying.
- Know what to do if something online has upset you: talk to Childline or the Samaritans if you are feeling desperate or sad, B-eat for eating disorder advice and Report-it to report incidents of race hate.

Shopping and Commerce

What is commerce?

Online shopping brings the High Street to your fingertips, wherever you are. The internet offers great choice and shopping online can be really convenient – there are no closing times, or queues, and you can compare deals from dozens of online stores to get the best deals. There are also other forms of shopping that are unique to the internet. For example, you can pay for virtual goods and services using virtual currency to spend in games on social networking sites. But while online shopping can bring many benefits, there are also some risks. Below are a few things you need to look out for when shopping online – and a few steps you can take to ensure that you are not left out of pocket.

Things to think about

- Remember – if an offer seems too good to be true, it probably is
- It's also a good idea to look for unbiased reviews of online retailers. Cross check information on the internet and see if anyone else has had problems.
- Beware of online scams, which can be very convincing; check that online stores have a physical address and telephone contact details

Things to do

- Buy from reputable retailers online – brands and services you know well in person, or which you have researched thoroughly
- When paying for goods and services online, make sure that the web address in the browser begings with https:// - the 's' stands for secure and ensures that any personal and financial data cannot be intercepted during transactions.
- Look for the padlock symbol on payment pages. Don't be fooled by a padlock that appears on the web page itself. It's easy to copy the image of a padlock. You need to look for one that is in the window frame of the browser itself
- Always use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared a password in the past, change it). An example would be 1%43?Owl765HP.
- Never follow links to shopping or banking sites – always type the address straight into the address bar

- Tell the truth about your age and do not lie about it to obtain goods or services which are age restricted – if you do you will be breaking the law
- Remember to always log out of a service properly after use, especially on a shared computer

Additional advice for parents and carers

- Ensure that you and your children check for the padlock symbol in the window frame of the browser; only 25% of 12-15s do this when visiting new sites according to Ofcom
- Talk to your children about safe online shopping and supervise purchases with younger children – explain that criminals can set up online shops that are only there to steal money, so check out the website carefully, e careful when disclosing any personal/financial/payment information and ensure that the site is using a secure payment method
- Check bank and card transactions regularly for unrecognised transactions
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date – security software provided by your internet service provider or third party can tell you whether a site is secure or not

Reporting

- You can report fraud or online scams or viruses to Action Fraud – the UK's national fraud reporting centre
- Get Safe Online provides advice on how people can use the internet confidently, safely and securely.