

eSafety Policy

HOW TO BE SAFE ONLINE IN EDUCATION

Christian Brothers
Grammar School,
Omagh

Contents

Aims	2
Risks	2
Roles and Responsibilities.....	3
Policy Decisions.....	7
Expected Conduct	8
Incident Management.....	9
Cyber-Bullying.....	10
eSafety Education and Curriculum.....	15
eSafety and Teaching and Learning	18
eSafety and E-mail	20
eSafety and Internet security.....	22
eSafety and Network management (user access, backup).....	24
eSafety and the School Website	26
eSafety and Digital Content - Digital images and video.....	26
How can emerging technologies be managed for eSafety?	27
Personal Electronic Devices	27
eSafety and our Virtual Learning Environment	28
eSafety and Social networking.....	29
Data security: Management Information System access and Data transfer	30
Useful Resources.....	31
Helpful Checklists.....	32
eSafety Advice.....	33

Aims

The aim of our eSafety policy is to outline the procedures that we have put in place to ensure that our pupils and staff can make best use of the ICT facilities available to them in a safe and secure way.

eSafety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

The eSafety Policy is part of the ICT Policy and School Improvement Plan and relates to other policies including those for behaviour and Wellbeing. This policy refers to the pupil and staff AUP (Acceptable Use Policy (of the network and services) and also the Data Security Policy which should be read in conjunction with this policy.

Risks

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, online gambling and financial scams
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including hacking social media profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
(Ref Ofsted 2013)

Roles and Responsibilities

The School's eSafety Coordinator is Mr N Donnelly, who will work closely with the Head of Wellbeing Mr A White and the Head of ICT Mrs S McLaughlin to co-ordinate eSafety awareness training and publication of resources.

The Head of Wellbeing who is the school's Designated Teacher for Child Protection, should be informed promptly of any disclosures, incidents or concerns of a safeguarding nature which will be dealt with in accordance with the school's Child Protection Policy. In the absence of the school's Designated Teacher for Child Protection, matters should be referred to one of the Deputy Designated Teachers.

The Senior Leadership Team and Board of Governors must be involved and should review the eSafety policy annually in conjunction with an Incident log, and monitor its impact. They will also need to ensure that they take responsibility for revising the eSafety policy and practice where necessary (such as after an incident or change in national legislation).

The Principal and Board of Governors have a legal responsibility to safeguard children and staff and this includes online activity.

All students have eSafety awareness as a part of their induction and both the ICT and LLW departments cover how to be safe online in their curriculums. We will organise assemblies and workshops with our students and teachers to highlight the safe and prudent use of online services.

This eSafety Policy has been written by the school, to build on the AUP policy and government guidance. It will be reviewed annually, involving staff and the Staff Council; Students and the Student Council; Parents and Parents' Council; management and the Board of Governors.

Governors	<ul style="list-style-type: none"> • To ensure that the school follows all current eSafety advice to keep the children and staff safe and ensure that a comprehensive and up to date eSafety Policy is in place • To approve the eSafety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in eSafety activities
The Principal	<ul style="list-style-type: none"> • To take overall responsibility for eSafety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their eSafety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious eSafety incident. • To receive regular monitoring reports from the eSafety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal eSafety procedures (e.g. network manager)
Head of Wellbeing	<ul style="list-style-type: none"> • To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafety incident which has implications for the safety and wellbeing of a child; • Facilitates training and advice for all staff <ul style="list-style-type: none"> ○ On how to deal with an eSafety incident, applying the procedures set out in the school's Child Protection Policy. ○ On the school's Code of conduct as set out in Appendix iv of the school's Child Protection Policy • Liaises with the WELB and relevant agencies for advice and guidance when dealing with an eSafety incident • Is regularly updated in eSafety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> ○ sharing of personal data ○ access to illegal / inappropriate materials ○ inappropriate on-line contact with adults / strangers ○ potential or actual incidents of grooming ○ cyber-bullying and use of social media

<p>Services Manager</p>	<ul style="list-style-type: none"> • To report any eSafety network related issues to the Services Manager. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • Risk Assessment of new technologies • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • That he / she keeps up to date with the school's eSafety policy and technical information in order to effectively carry out their eSafety role and to inform and update others as relevant • That the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the HoSL for investigation / action / sanction and referred on if necessary • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures • To ensure that all data held on pupils on the school's management information system is only accessed by those authorised to view the data.
<p>Head of eLearning</p>	<ul style="list-style-type: none"> • Takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies / documents • Promotes an awareness and commitment to e-safeguarding throughout the school community • Evaluates effective eSafety education, embedded across the curriculum and liaises with IT Services staff to ensure support and review of same • To report any eSafety related issues that arise, to the Services Manager and relevant HoSL. • To communicate regularly with SLT and the designated eSafety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • Organises training for staff on the eSafety awareness and etiquette in light of the introduction and use of new technologies
<p>Head of ICT</p>	<ul style="list-style-type: none"> • To oversee the delivery of the eSafety element of the ICT curriculum • To liaise with the Head of eLearning regularly in the review of eSafety in the curriculum and effects of new technologies within teaching
<p>Teachers</p>	<ul style="list-style-type: none"> • To embed eSafety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the HoSL • To maintain an awareness of current eSafety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. non-school email accounts, text, mobile phones, non-school social media platforms etc. in line with the guidance set out in the Code of conduct
Pupils	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Student Acceptable Use Agreement / Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand and abide by the school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand and abide by the school policy on the taking / use of images and on cyberbullying. • To understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the review of eSafety policy
Parents / Guardians	<ul style="list-style-type: none"> • To support the school in promoting eSafety • Read, understand and sign the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's provision of ICT facilities including a VLE • To promote the school Pupil Acceptable Use Agreement with their children • To access the school website / VLE / SIMS Learning Gateway etc in accordance with the relevant school procedures and policies. • To consult with the school if they have any concerns about their children's use of technology

Policy Decisions

How will online access be authorised?

- The School maintains a current record of all staff and pupils who are granted access to the School's electronic communications. All staff must read and sign the 'Staff Information AUP' before using any School ICT resource.
- All pupils agree to abide by our Acceptable Use Policy each time they login.
- The eSafety policy and AUP will now be given out when they register.

How will risks be assessed?

- As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The School recognises the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the School system. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer.
- The School audits ICT use to establish if our eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.
- In order to ensure that students are equipped to make safe decisions about their time online when away from school (where the filters and firewalls may not be as robust) curriculum time is devoted to teaching safe searching and assessing the risks of sharing data so students can make good decisions.

How will eSafety and Cyber Bullying complaints be handled?

- Complaints of Internet misuse will be dealt with in accordance with school policies. Any issues of eSafety regarding pupils will be dealt with by the relevant manager.
- Any issues relating to breach of the Acceptable Use Policy will be dealt with by the Head of Student Learning and the Services Manager. Any complaint about staff misuse will be referred to the Principal.
- Sanctions regarding cyber-bullying are outlined in the School's anti-bullying policy
- Sanctions for breach of the AUP range between temporary removal of Internet access to temporary exclusion depending on the severity of the offence

Expected Conduct

All users

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices i.e. Electronic Devices Policy. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- are responsible for reading the school's eSafety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and the school's policies on Coursework and Electronic Devices

Parents/Guardians

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the eSafety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

- There is strict monitoring and application of the eSafety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (eg the WELB, C2K, UK Safer Internet Centre helpline) in dealing with eSafety issues
- Monitoring and reporting of eSafety incidents takes place and contribute to developments in policy and practice in eSafety within the school. The records are reviewed and reported to the school's senior leaders, Governors
- Parents / guardians are specifically informed of eSafety incidents involving young people for whom they are responsible.

Introduction

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other eSafety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Rationale

- The cyber world opens up immense opportunities for children and adults. It is integral to modern day youth culture and to the world of work. However it also carries many threats. The school wants to equip staff with an understanding of the risks of new technologies and how to prevent, recognise and respond to them.
- This policy aims to ensure that children are safe and feel safe from bullying, harassment and discrimination. This school is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly.
- The rapid development of, and widespread access to, technology has provided a new medium for bullying, which can occur in or outside school. Cyber-bullying is a form of bullying which can happen 24/7, with a potentially bigger audience and more accessories as people forward on content at a click.
- The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The development and implementation of this policy has involved all the stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents and the students themselves.

Aims of eSafety Policy in dealing with Cyberbullying?

- To ensure that students, staff and parents understand the concept of cyber bullying and how it can be combated effectively and quickly.
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying and to promote eSafety.
- To understand how to minimise the risk to children using the internet. To develop an awareness and understanding of the legislative context for safeguarding children in a digital world.
- To consider elements of good practice to keep children safe when using the internet.
- To understand the role and remit of staff in different services linked to eSafety.

What is Cyberbullying?

A short definition of cyberbullying is: “using technology as a weapon to intentionally target and hurt another person, it’s ‘cyberbullying.’”

- Cyber bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including pupils and school staff.

It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication or forwarding of private information or images with malicious content.

Procedures to Prevent Cyber bullying

- Staff, student, parents and governors to be made aware of issues surrounding cyber bullying and eSafety.
- Students and parents will be urged to report all incidents of cyber bullying to the school. Staff CPD will assist in learning about current technologies
- Students will be involved in developing and communicating this policy. Students will learn about cyber bullying through curriculum, assemblies, anti-bullying week activities, ‘Safer Internet Day’ ([Safer Internet Day 2016 – 9th February 2016](#)) and other curriculum projects.
- Students and staff will sign an ‘Acceptable Use of ICT’ contract.
- Parents will be provided with information and advice on how to combat cyber bullying.
- Parents will be expected to sign an ‘Acceptable Use of ICT’ contract and to discuss the details of this document with their children.
- Students, parents and staff will be involved in reviewing and revising this policy and school procedure.
- All reports of bullying including cyber bullying will be investigated, recorded and monitored with in accordance with school policies.
- The WELB can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents.
- If appropriate the police will be contacted in cases of actual or suspected illegal content.

Sanctions

At Christian Brothers Grammar School, Omagh, we take this bullying as seriously as all other types of bullying and therefore, will deal with each situation individually. An episode may result in a range of interventions, including verbal warnings and involvement of parents. Clearly, more serious cases will result in further sanctions. Sanctions for all types of bullying are applied through our Positive Behaviour policy.

- The school believes that all people in our community have the right to teach and learn in a supportive, caring and safe environment without fear of being bullied. We believe that every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.
- Procedures for reporting bullying can be found in the Anti-bullying policy and the Positive Behaviour Policy.

Support

- Technology allows the user to bully anonymously or from an unknown location, 24 hours a day, 7 days a week. Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher but is highly intrusive and the hurt it causes can be very severe.
- Young people are particularly adept at adapting to new technology, an area that can seem a closed world to adults. For example, the numerous acronyms used by young people in chat rooms and in text messages (POS - Parents Over Shoulder, TUL – Tell You Later) make it difficult for adults to recognise potential threats.
- Christian Brothers Grammar School, Omagh, has an 'Acceptable Use Policy' (AUP) that includes clear statements about e-communications.



If you or someone you know is a victim of cyber bullying please contact a member of staff

Support for parents

- Information for parents on e-communication standards and practices in schools
- What to do if problems arise
- Information on what is being taught in the curriculum.
- Support for parents and students if cyber bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence.

Student Support

Students are taught how to:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them.
- Know what to do if they or someone they know are being cyberbullied.
- Report any problems with cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to take appropriate action.

Key Web Links

- More information for parents, guardians and young people can be found on the government website www.thinkuknow.co.uk.
- If you are a young person, parent or guardian and need to report a problem you can do so at: http://www.ceop.gov.uk/ceop_report.aspx
- There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips.

Who to contact

- Students who experience cyber bullying can contact Mr A White, their Form Teacher or Head of Student Learning. If the cyber bullying has occurred outside of the school environment, then students are advised to speak to their parent/guardian immediately.
- Staff should contact the relevant Head of Student Learning directly, who will liaise with Mr A White. Mr A White has responsibility for all anti-bullying initiatives.
- School Counsellor – self referral system.

Our defence against cyber-bullying

New communications technologies offer anonymity, due to this anyone with a mobile phone or Internet connection can be a target for cyber bullying. What's more, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. This is simply bullying and sanctions for such activities will be serious and guidelines can be seen in the Behaviour policy.

Most cyber bullying is done by students in the same class or year group. Although it leaves no visible scars, cyber bullying of all types can be extremely destructive.

What young people said would help

<http://nobullying.com/cyberbullying-bullying-statistics-2014-finally>

- 7 in 10 young people are victims of cyberbullying.
- 37% of them are experiencing cyberbullying on a highly frequent basis.
- 20% of young people are experiencing extreme cyberbullying on a daily basis.
- New research suggests that young males and females are equally at risk of cyberbullying.
- Young people found to be twice as likely to be cyber bullied on Facebook as on any other social network.
- 54% of young people using Facebook reported that they have experienced cyberbullying on the social network.
- Facebook, Ask.FM and Twitter found to be the most likely sources of cyberbullying, being the highest in traffic of all social networks.
- Cyberbullying found to have catastrophic effects upon the self-esteem and social lives of up to 70% of young people.
- An estimated 5.43 million young people in the UK have experienced cyberbullying, with 1.26 million subjected to extreme cyberbullying on a daily basis.

The law is on your side

The following laws may be used to combat cyber bullying. People may be fined or sent to prison for up to six months.

- The Protection from Harassment Act,
- the Malicious Communications Act 1988 and
- Section 43 of the Telecommunications Act

Our website and eSafety

We have a dedicated eSafety section on the school's website.

- This section includes guidance videos for both students and parents on safer internet use with links to the Child Exploitation and Online Protection Agency websites.
 - <https://www.thinkuknow.co.uk>
 - <http://ceop.police.uk/>
- We also have a safeguarding area of the website for parents specifically.
 - This area contains a list of important contacts at the school for parents and guardians as well as links & contact information for organisations such as the NSPCC.
- This policy and the Anti-Bullying policy can be found in these sections.

Student ICT network and eSafety resources

- Once logged onto the schools network, all students have a link to the Child Exploitation and Online Protection Agency websites.
 - <https://www.thinkuknow.co.uk>
 - <http://ceop.police.uk/>
- eSafety and cyberbullying are also covered in the ICT and Life Skills curricula.

Remote working

All students at Christian Brothers Grammar School, Omagh, have the capability to work remotely from home through a remote access solution provided by the school. Before students can use this system they must:

- Have read and signed the Student Acceptable Use Policy.
- Be aware that activity will be logged while working remotely
- Be subjected to the same internet filtering limitations

Three helpful steps to stay away from harm

- Respect other people - online and off. Don't spread rumours about people or share their secrets including their phone numbers and passwords
- If someone insults you online or by phone, stay calm – and ignore them.
- Do as you would be done by. Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by somebody else

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

Pupil eSafety curriculum

Christian Brothers Grammar School, Omagh has a clear, progressive eSafety education programme as part of the ICT curriculum and Life Skills curricula. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- to understand why and how some people will 'groom' young people for sexual reasons;
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies,
 - i.e. parent or guardian, teacher or trusted staff member, or an organisation such as Childline or the CEOP.
- To plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
- Ensure that staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in:
 - pop-ups;
 - buying on-line;
 - on-line gaming / gambling

How will the policy be introduced to pupils?

eSafety is a crucial part of every pupils' education at the School. Currently the following are used to ensure pupils are aware of the issues:

- At least one assembly for each year group per year is on the topic of eSafety
- A summary of the key points from the School AUP is displayed each time pupils log in
- The eSafety policy is available via the School's website
- Links to various eSafety websites are on the School website
- Parents' Evenings will include publications and promotions on the topic of eSafety
- Posters around the School highlighting eSafety

Staff and Governor training

- Christian Brothers Grammar School, Omagh ensures all staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on eSafety issues and the school's eSafety education program; annual updates/ staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafety Policy and the school's Acceptable Use Policies.

How will the policy be discussed with staff?

- The eSafety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- All staff will be made aware of the electronic version of the School eSafety Policy and its application and importance explained.
- Staff are made aware that Internet traffic is be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues. All breaches of eSafety policy should be reported to the HoSL
- Staff training in safe and responsible Internet use and on the School eSafety Policy will be provided as required.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

Parent awareness and training

A partnership approach with parents is encouraged. Christian Brothers Grammar School, Omagh runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
 - Parents will be requested to read the school's e-Safety/Internet agreement as part of the Acceptable Use Policy.
 - Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.

 - Parents' attention will be drawn to the School's eSafety Policy in publications and on the School website.
 - demonstrations, practical sessions held at school;
 - suggestions for safe Internet use at home;
 - provision of information about national support sites for parents.

 - Internet issues will be handled sensitively, and parents will be advised accordingly.
 - Information and guidance for parents on e-Safety, as well as advice on useful resources and websites, which include responsible use of the Internet, will be made available to parents on the school website.

 - The school's Parents' Council will review this Policy and provide feedback.
-

Why is Internet use important?

- The purpose of Internet use in the School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. Christian Brothers' Grammar School, Omagh has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and sources and critically, to take care of their own safety and security.

How does Internet use benefit education?

- Benefits of using the Internet in education include:
 - Access to world-wide educational resources in their various multimedia formats;
 - Inclusion in the National Education Network which connects all UK schools;
 - Educational and cultural exchanges between pupils world-wide;
 - Vocational, social and leisure use in libraries, clubs and at home;
 - Access to experts in many fields for pupils and staff;
 - Professional development for staff through access to national developments, educational materials and effective curriculum practice;
 - Collaboration across support services and professional associations;
 - Improved access to technical support including remote management of networks and automatic system updates;
 - Exchange of curriculum and administration data between Christian Brothers' Grammar School, Omagh, Omagh Learning Community, the WELB and Department of Education;
 - Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Christian Brothers' Grammar School, Omagh aims to develop effective practice in Internet use for teaching and learning. Teachers and support staff help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites. Internet searching skills is part of the ICT curriculum. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- The School Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are explicitly taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. The Services Manager will contact the eSafety Co-ordinator to oversee requests in this regard?
- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The ICT KS3 curriculum will enable students to become mature internet users by incorporating all the above.
- The Life Skills curriculum assists students in assessing risk in handling and sharing their personal information online as well as the meaning and consequences of cyber-bullying.

Christian Brothers Grammar School, Omagh

- Provides staff with a C2K email Account for their professional use, and makes it clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@cbs.omagh.ni.sch.uk or potentially department / class e-mail addresses for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is in breach of the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Agencies and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of C2K-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Websense monitors and protects our internet access to the World Wide Web.
-

Pupils:

- We use C2K email with pupils and lock this down where appropriate using C2K rules.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e.:
 - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/guardian;
 - that an e-mail is a form of publishing where the message should be clear, short and concise;
 - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
 - must not reveal private details of themselves or others in e-mail, e.g. address, contact number, etc;
 - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
 - that they should think carefully before sending any attachments;
 - embedding adverts is not allowed;
 - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
 - not to respond to malicious or threatening messages;
 - not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
 - not to arrange to meet anyone they meet through e-mail and discuss this with an parent/guardian and teacher if someone suggests such a meeting;
 - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the Student Acceptable Use Policy to say they have read and understood the eSafety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use C2K e-mail systems for professional purposes
 - Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
 - the sending of chain letters is not permitted;
 - embedding adverts is not allowed;
 - All staff sign our Staff Acceptable Use Policy to say they have read and understood the eSafety rules, including e-mail and we explain how any inappropriate use will be dealt with.
-

Christian Brothers Grammar School, Omagh

Anti-virus and Encryption

- Has the educational filtered secure broadband connectivity through C2K
- BT.NET and the CBS Network
 - Uses the Websense filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
 - All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved C2K secure system;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level / appropriate standards suitable for educational use;
- Uses C2K secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;

Appropriate Access

- Ensures pupils only publish within an appropriately secure environment : the school's learning environment, secure platforms such as provided by C2K; e.g. 'MySchool'
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
 - Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;

Supervision and acceptable use

- Informs all users that Internet use is monitored;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google / Bing image search;
- Staff will use software (Impero) in ICT rooms to monitor pupil's usage of internet.

Monitoring and Reporting

- Works in partnership with C2K to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Services Manager;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the WELB.

eSafety and Network management (user access, backup)

Christian Brothers Grammar School, Omagh

- Uses individual, audited log-ins for all users – within the CBS Network and the C2K system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites
- Has additional local network auditing software installed;
- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

Ensuring the network is used safely

Access and logons

- Ensure staff read and sign that they have understood the school's eSafety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a username for access to our school's CBS network;
- Staff access to SIMS is controlled through a separate password for data security purposes;
- We provide pupils with an individual CBS Network log-in username. They are also expected to use a personal password;
- All pupils have their own unique C2K username and password which gives them access to the MySchool Learning Platform and their own school approved email account;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has integrated curriculum and administration networks, but access to SIMS is set-up so as to ensure staff users can only access modules related to their role;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / C2K approved systems: e.g. 'MySchool';
- Provides pupils and staff with access to content and resources through MySchool which staff and pupils access using their username and password;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers are provided with attendance data on specific children, parents using a secure portal to access information on their child;

Logging off and shutting down terminals

- Requires all users to always log off when they have finished working or are leaving the computer unattended;
 - Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.

Restrictions

- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

Backups

- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;

Health and Safety

- Reviews the school ICT systems regularly with regard to health and safety and security and ensures all computer equipment is installed professionally and meets health and safety standards;
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by Services Team; equipment installed and checked by approved Suppliers / electrical engineers

Passwords policy

Christian Brothers Grammar School, Omagh makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find;

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We advise staff to use strong passwords for access into our SIMS system.
- We require staff to change their passwords into MySchool twice a year

eSafety and the School Website

- The Services Manager takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@cbs.omagh.ni.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web are consistent with parental consent
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.
- We have an eSafety section with advice and links to policies and resources.

eSafety and Digital Content - Digital images and video

In Christian Brothers Grammar School, Omagh;

- We gain parental / guardian permission for use of digital photographs or video involving their child as part of the school agreement form when their son joins the school;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school has obtained individual parental or pupil permission for its long term use
- Staff and pupils sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils consistent with the school's Electronic Devices Policy;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school.
- We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Pupils will not take any photographs or video footage unless under the supervision of a member of staff (i.e. Media Studies, Performing Arts etc)

How can emerging technologies be managed for eSafety?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Lync, Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

Video Conferencing

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

Christian Brothers Grammar School, Omagh

- Only uses the C2K/DE supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

Personal Electronic Devices

- Personal Electronic Devices will not be used by pupils during lessons or formal school time, unless part of their lesson. Teachers wanting to use mobile phone technology in their lesson must, like students, operate within the guidelines of the Personal Electronic Devices Policy.
- The sending of abusive or inappropriate text messages is forbidden and covered in the school's Positive Behaviour Policy as bullying.
- Staff will be issued with a School phone where contact with pupils is required. Staff must not give their personal mobile number to pupils.

eSafety and our Virtual Learning Environment

How will Learning Platforms be managed?

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure ePortfolios to showcase examples of work.

Access and Resources

- Pupils/staff will be advised about acceptable conduct and use when using the Learning Platform.
- Only members of the current pupil, parent/guardians and staff community will have access to the Learning Platform.
- A visitor may be invited onto the Learning Platform as approved by the Head of eLearning. In this instance there may be an agreed focus or a limited time slot.
- Uploading of information on the schools' Virtual Learning Environment is shared between different staff members according to their responsibilities e.g. all departments upload information in their department areas;
- Photographs and videos uploaded to the schools Virtual Learning Environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as those accessed within 'MySchool';
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled.

Dealing with Concerns

- Any concerns about content on the Learning Platform may be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - The material will be removed by the site administrator if the user does not comply.
 - Access to the Learning Platform for the user may be suspended.
 - The user will need to discuss the issues with a member of Management before reinstatement.
 - A pupil's parent/guardian may be informed.

eSafety and Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' 'MySchool' Services for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / parents / guardians or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students will ensure that in private use:

- No reference should be made in social media to fellow students / parents / guardians or school staff

Data security: Management Information System access and Data transfer

Strategic and operational practices

Christian Brothers Grammar School, Omagh:

- The Services Manager, Mr D Hunter, manages the school network
- Staff are clear who are the key contact(s) for key school information are. We have listed the information and information asset owners in a spreadsheet.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff have personnel records held in one central record in SIMS
- We ensure all the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
 - staff,
 - governors,
 - pupils
 - parents
- This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow DE guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the WELB or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Appendix A

Useful Resources

Helpful Checklists

DOWNLOADS

- [Instagram Safety Checklist](#)
- [Facebook Settings Checklist](#)
- [Snapchat Checklist](#)
- [Twitter Checklist](#)
- [Guidelines on AskFM](#)

Follow these tips for greater social media privacy:

Facebook – remove unwanted tags from multiple photos

- Go to your activity log
- Click 'Photos' in the left column
- Select the photos from which you'd like to remove a tag; click 'Report/remove tags'
- Click 'Untag photos'
- Removed tags will no longer appear on the post or photo will still be visible to the audience it's shared with.
- Coconnectsafely.org's – [A Parent's Guide to Facebook](#)

Twitter – Protect tweets so that only your followers can see them

- Go to your account's 'Security and privacy' settings
- Scroll down to the 'Tweet privacy' section and check the box next to 'Protect my tweets'
- Click the blue 'Save' button at the bottom of the page. You will be prompted to enter your password to confirm the changes.

Instagram – Set photos to private so only your followers can see them

On iOS

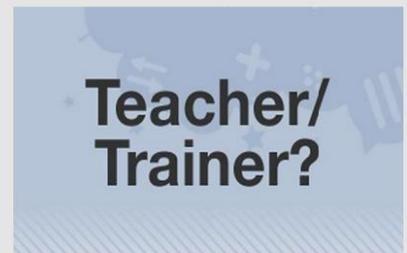
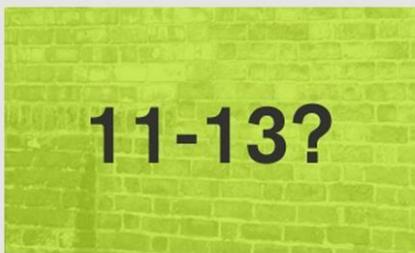
- Tap 'Edit your profile' next to your profile picture
- Turn on the 'Posts are private' setting and then tap 'Done'
- If you have an android phone, tap the check mark instead to save your changes.



Welcome to CEOP's Thinkuknow

Come in to find the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there's an area for you too – with resources you can use in the classroom or at home. Most importantly, there's also a place which anyone can use to [report](#) if they feel uncomfortable or worried about someone they are chatting to online. All the information here is brought to you by the team at the [NCA's CEOP Command](#). We hope you like it!

Are you...



Ever posted something you regret? Find out how to get help when things go too far. You choose what happens in this interactive film!

[Watch First to a Million now!](#)



Advice... Help... Report...

Specifically has sections for parents of Secondary Children

THINK UK KNOW
co.uk

Home
Primary
Secondary
What is my child doing online?
Conversation Starters
Risks my child might face
Tools to protect my child
Talk to your child about...Webcams
Advice for carers
Advice for Adoptive Parents
The Parents' and Carers' Guide
Keeping up with the Joneses
Visa

CLICK CEOP
Internet safety port

Browser Safety
download the ClickCEOP tools available for your browser.
Now in...
Windows Internet Explorer 9

Follow Us
Follow @ceopuk 14.2K followers

Password: Sign In
Forgot Password? | Register

Growing up online

As your child grows and becomes more independent, it is only natural that they take this independence online. In our teenage years we explore, try new things and sometimes push boundaries and take risks, this is an essential part of growing up.

With all of the potential that the online world and new technology offers, young people now have access to huge opportunities. They use technology to express themselves, explore, and be creative; it has changed the way they communicate.

The internet has changed all of our lives, and your child has grown up during this change. Many of the things that confuse, baffle or even scare us, are part of the everyday for them. For many of us, this can all be a bit too much.

Whether you're a technophobe or a technophile, it's still likely that you'll be playing catch-up with the way your child is using the internet.

You might wonder whether what they are doing is safe, and you might also be thinking *how can I be as good a parent online as I am offline?*

This site aims to make online parenting simple.

- What is my child doing online?
- How do I talk to my child about what they're doing online?
- What risks might my child face?
- What tools are there to help me keep my child safe?

Top Tips

- **Be involved in your child's online life.** For many of today's young people there is no line between the online and offline worlds. Young people use the internet to socialise and grow and, just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support. **Tips on how to discuss tricky issues with your child**
- **Watch Thinkuknow films to learn more.** The Thinkuknow programme has **films and advice for children** from five all the way to 16. Your child may have seen these at school, but they can also be a good tool for you to find out more about what young people do online and some of the potential risks.
- **Keep up-to-date with your child's development online.** Be inquisitive and interested in the new gadgets and sites that

E-SAFETY IN THE COMPUTING CURRICULUM

Unsure about how to teach e-safety in the new Computing curriculum?
Click here to check out our guides for Key Stages 1 to 4.

Welcome to Childnet International, a non-profit organisation working with others to help make the internet a great and safe place for children.

Twitter @childnet



about a day ago

RT @samsantics2: @childnet now have resources #supportingyoungpeopleonline in a no of different languages - from Arabic to Vietnamese [http...](#)



about 2 days ago

#ff to our #Digiduck creators @Lins_Buck & @tinyflood and our supporters @MicrosoftUK & @IM_org <http://t.co/Y7bidBf14w>



Young people

Top tips, games and internet safety information to help young people get the very best out of the internet and stay safe online.



Teachers and Professionals

Internet safety resources for teachers and professionals to help safeguard your workplace and the young people you work with.



Parents and Carers

Advice for parents and carers to help support children and young people in their safe and responsible use of the internet.

KidSMART I work with kids I have kids Contact

What's your favourite thing to do online? Learn more about the internet and being a SMART surfer here!

BEING SMART RULES

MOBILES CHAT SAFE SEARCHING

FILE SHARING SOCIAL NETWORKING DIGITAL FOOTPRINTS

GREAT SITES MUSIC GAMES GALLERY COMPETITIONS

SKILLS SCHOOL NEW! NETWORKERS

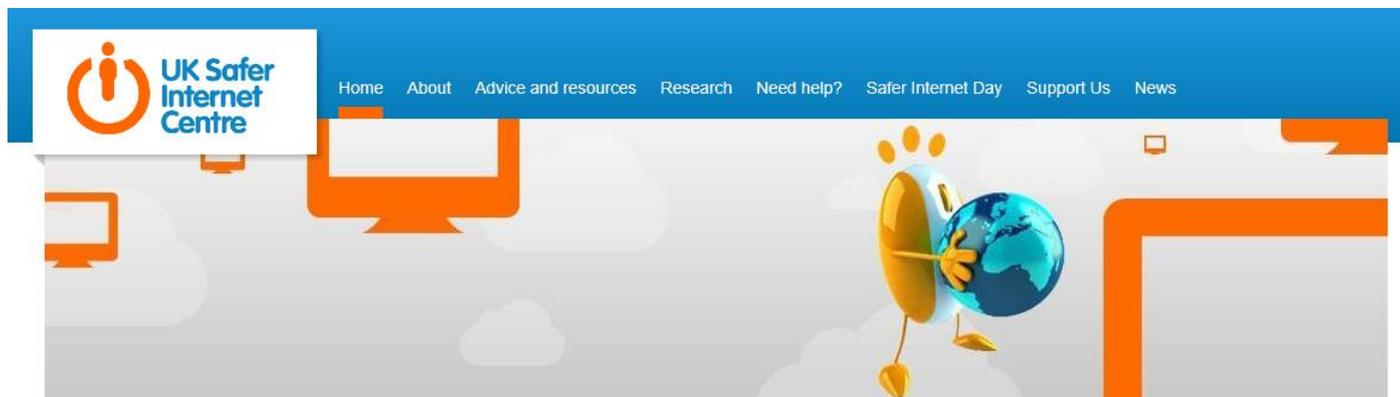
NET NASTIES

Make your join hands person and share your advice! Remember meeting up with online friends can be

Some other useful sites:

digizen.org Know IT All for Secondary Schools CHALLENGE UK Safer Internet Centre SOCIAL NETWORKING SITES THINK U KNOW

Including resources for Safer Internet Day



Welcome to the UK Safer Internet Centre, where you can find e-safety tips, advice and resources to help children and young people stay safe on the internet.

Twitter @UK_SIC

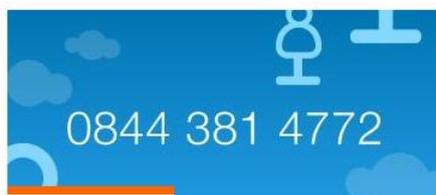
 about 2 days ago
11-18 year olds it only takes 10 minutes to complete @childnet's survey about apps & mobiles! buff.ly/1J9kXi3
pic.twitter.com/jmV9ux7ne0

 about 3 days ago
How young people are shaping @childnet's new #cyberbullying project buff.ly/1QSZINV pic.twitter.com/bl8e4JPucz



Safer Internet Day

Safer Internet Day 2016 will take place on 9th February 2016. Find out more and get involved!



Helpline

0844 381 4772

The UK Safer Internet Centre's helpline for professionals working with young people in the UK.



Hotline

The UK Safer Internet Centre's hotline for the public to report online child sexual abuse content.



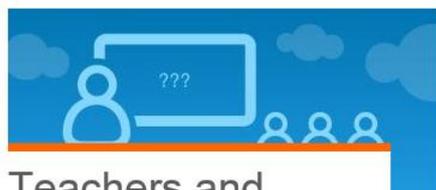
Young people

Games, films, quizzes and advice to help you stay safe online. With resources for primary and secondary age children.



Parents and carers

Advice about key esafety topics like social networking, as well as how-to guides for setting up filters and parent settings.



Teachers and professionals

Educational resources, e-safety policy and protecting your online reputation - for teachers, social workers and more.

<http://www.saferinternet.org.uk/advice-andresources/parents-and-carers/parental-controls>

Parental controls offered by your home internet provider

How to set up filters on your home internet to help prevent age inappropriate content being accessed on devices in your home.

The 4 big internet providers in the UK – BT, Sky, TalkTalk and Virgin Media - provide their customers with free parental controls which can be activated at any time. They have come together to produce these helpful video guides to help you to download and set-up the controls offered by your provider.



How to set up the parental controls offered by BT



How to set up the parental controls offered by Sky

Young people
Parents and carers
Have a conversation
Safety tools on online services
Parental controls
Parents' Guide to Technology
Teachers and professionals

Insafe Tip Sheets -

<http://www.saferinternet.org/tipsheets>

HOME | ONLINE ISSUES | RESOURCES | COUNTRIES | SAFER INTERNET DAY | NEWS & EVENTS

Search...

insafe

f | t | v | You Tube

INSAFE TIP SHEETS

Insafe has developed a range of tip sheets to help you learn more about the tools and services you might be using online, and how to protect your privacy while doing so. Click on the links to the right to access and download them.

We aim to update these sheets regularly and add to them with new topics as and when they emerge. If there is a particular topic or app you would like to see covered, please let us know.



DOWNLOAD INSAFE TIP SHEETS...

- > ask.fm
- > Chatbot mobile apps (NEW March 2014)
- > In app purchases
- > Instagram - for Android devices
- > Instagram - for Apple devices
- > Snapchat
- > Twitter
- > Tumblr
- > WhatsApp

UK Safer Internet Centre

Home About **Advice and resources** Research Need help? Safer Internet Day Support Us News

Parents' Guide to Technology

In the parents' sessions we run in schools, we get a lot of questions about particular devices that children are using or asking for. This guide has been created to answer these questions and introduce some of the most popular devices, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly.

Smartphones

This includes: BlackBerry, iPhone

Gaming devices

This includes: Xbox 360, PlayStation 3, PSP, Nintendo Wii, Nintendo 3DS, Nintendo DSi

Young people

Parents and carers

- Have a conversation
- Safety tools on online services
- Parental controls
- Parents' Guide to Technology**
- Smartphones
- Gaming devices
- Internet-enabled devices

Teachers and professionals

Foster carers, adoptive parents and social workers

Quick downloads:

Download our top tips for iPhone PDF

+ see our updated guides for the iPad, iPod Touch and our newest guide for the Kindle Fire

Child Exploitation and Online Protection Agency (CEOP)

<http://ceop.police.uk/>

The screenshot shows the CEOP Command website homepage. At the top left is the CEOP logo with the text 'A National Crime Agency command'. To its right is the 'CEOP Command' title and navigation links: Home, About CEOP, Media Centre, Education, Publications, Partners and Supporters, Recruitment, and Contact us. On the top right, there are social media icons for Facebook and Twitter, and a red button that says 'Advice.. Help.. Report..' with the 'CLICK CEOP Internet safety' logo below it. The main banner features a line-art illustration of a laptop with the 'CLICK CEOP Internet Safety' logo on the screen, surrounded by various electronic devices. A dark blue box over the banner contains the text: 'For advice, help or to make a report visit our safety centre'. Below the banner are three sections: 'Our sites' with logos for 'THINK UK KNOW', 'mk UK', and 'MOST WANTED'; 'Follow us' with social media icons for Facebook, Twitter, and YouTube; and a 'child rescue alert' section with a red circular logo and text: 'You can now pre-register to receive Child Rescue Alerts via text and email when the system launches in May 2014. Sign up now'. The main content area is divided into three columns: 'Latest Stats' with a graphic showing 'Number of children safeguarded 2006 - 2013' and a 'View latest statistics' link; 'Want to know how to use webcam safely?' with a link to download a 'Webcam with Confidence' factsheet; and 'Latest Announcements More...' with a date '18 September 2014' and a link to 'NCA statement on Project Spade More...'. Below these are 'Information for...' links for 'Parents, Carers and Guardians', 'Teachers and Educational Professionals', 'Law Enforcement', and 'Industry and Internet Service', as well as 'Children and Young People' and 'International Jurisdictions'. A 'Spotlight on Our Work' section highlights 'Our Work Overseas' and 'Related content' including 'CEOP Romania Bulgaria Video'. At the bottom left, it says 'Member Of' with logos for UKCCS and another organization.

This includes the CEOP alert link

If you are a young person, parent or guardian and need to report a problem you can do so by following this link:



CEOP Videos

CEOP 'The Parents' and Carers' Guide to the Internet',

<http://youtu.be/YyzokhRfRJA> - this is a light hearted and realistic look at what it takes to be a better online parent. The show covers topics such as, talking to your child about the technologies they use and the things they might see, such as pornography.

Consequences: Assembly for 11 16 year olds

<http://youtu.be/hK5OeGeudBM> - This is an assembly from CEOPs Thinkuknow education programme that enables young people to recognise what constitutes personal information. The assembly facilitates young people's understanding that they need to be just as protective of their personal information online, as they are in the real world. It also directs where to go and what to do if young people are worried about any of the issues covered.

Exposed

http://youtu.be/4ovR3FF_6us - This 10 minute drama has been designed for 14 to 18 year olds. 'Exposed' deals with the subjects of sexting and cyberbullying, issues that teenagers commonly face.



Get started

Read our guidance to help you stay in control, whatever age your son or daughter is.



Get started

Digital Parenting checklists

The technology timeline for kids and teens is far from straightforward. Not every seven year old / 10 year old / 15 year old uses the same technologies – it depends on things like how mature they are, what their parents' views are and what devices they have access to at home, at school and at their friends' houses.

With this in mind, we decided not to divide all the contents of *Digital Parenting* by age group. But we do understand that it can be helpful to have specific advice by age, so we've pulled together some key action points to help your son or daughter enjoy their digital world and stay safer at various ages.

We've started with an 'essentials' checklist for parents of children of any age, which highlights the actions you should take for your whole family. Then we have suggestions for parents with children of different ages.

These are by no means definitive lists (the tech world moves far too quickly to be able to promise that!) but they're a good starting point. We hope you find them useful.

✔ 'Essentials' checklist

- ✔ **THINK** about how you guide your family in the real world and do the same in the digital world – don't be afraid to set boundaries and rules for your child from a young age
- ✔ **HAVE** a go at some of the technologies your son or daughter enjoys – play on the Wii together or ask them to help set you up on Facebook if you're not already a member

Web Super Skills cards



Use our Web Super Skills cards to help explain internet safety to younger children.

› Download cards

👤 'How to' guides

▶ **Talk to your child about staying safe on computers and mobile phones**

A guide to the various ways cyberbullying occurs and information on how parents and carers can reduce the risks for their children

▶ **Social networking sites**

What social networks are and how you can help your child use them safely

▶ **Illegal downloading and file sharing**

The risks facing both themselves and their parents if children download over the internet illegally or attempt to share files with others

▶ **Help your child enjoy the internet safely: Click Clever, Click Safe**

Three simple rules to teach your child so they can enjoy the benefits of the internet safely

▶ **Internet terms and language: a guide for parents**

A simple explanation of some of the terms used when talking about potential dangers online

▶ **Online gaming**

Information about the kinds of games your child is likely to play, age ratings and how to keep safe playing online

▶ **Keeping children safe online**

How you can help to make sure children are able to enjoy the benefits of the internet whilst managing the risks

Search this site

[Sign in](#) or [Register](#)

[About us](#) [Getting started](#) [Help & advice](#) [News & events](#) [Training & awareness](#) [Resources](#)

You and the Safe Network

Have a **question?** Need some **guidance?** We can help you

[Get started](#)

1 2 3 4

Explore the Safe Network



Be aware of the potential online risks to children & young people
Help children and young people understand the potential risks and encourage safe and responsible use of the internet.
[Online policies](#)
[Best safeguarding practice](#)



FREE online safeguarding checklist

Online self-assessment tool for safeguarding children and young people.



Case studies from voluntary sector groups

Different approaches other groups have taken in setting up safeguarding policies.



Working alone with children and young people?

Best practice advice for those working closely with children in voluntary groups.



Get your FREE safeguarding resource

Are they safe? resource is free and helps groups set up safeguarding measures.

Most popular

[Are they Safe? pack](#)

What's new

[DBS focus week webinars launched](#)
[Research shows 1 in 5 child deaths in](#)

Quick start

for parents or carers [Go](#)

The Safe Network

Tweets [Follow](#)

Safe Network @thesafenetwork 26 Sep
We're off for the #weekend back Monday. If you're worried about a child & need advice call @NSPCC 0808 8005000 buff.ly/1pvxMGw

Safe Network @thesafenetwork 26 Sep
#DBS Disclosure & Barring Service focus week starts Monday! Keep an eye on R website safenetwork.org.uk & @thesafenetwork for updates

Safe Network @thesafenetwork 26 Sep
Hello & #Welcomeaboard to our #Friday followers @ABkaratefitness @WaseemRiaz0 @WAMYouth @ecvys @Ulfilas @PaintyUK Have a nice day :-D

[Register now to access useful resources](#)

Safe Search for Kids – Powered by Google

<http://www.safesearchkids.com/>

SAFE SEARCH KIDS

The Google Search Engine for Kids
where Safe Search is always on

[Parental Control Software](#) | [Safe Image Search](#) 

Bookmark: 

Internet Safety Articles

- [Social Media Safety \(Parents\)](#)
- [Social Media Safety \(Teens\)](#)
- [Child Safety Kit Program](#)
- [Cyber Bullying Guide \(Parents\)](#)
- [Cyber Bullying Resource \(Kids\)](#)
- [Parental Control Software](#)
- [Safe Search in Schools](#)
- [Posting Pictures Online](#)
- [Cell Phone Safety Tips](#)
- [Safe YouTube Search](#)
- [Wikipedia for Kids](#)

SHARE 



Welcome to Safe Search for Kids, powered by Google

Safe Search for Kids is the *child friendly* search engine where safe search is always 'on'.

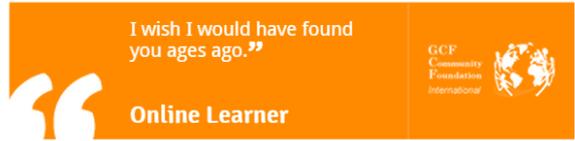
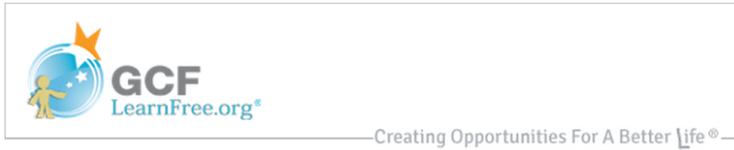
The safe browsing feature on this website overrides your computer search settings to help remove potentially explicit material when searching Google. No changes are made to your computer or your browser settings. Safe search happens automatically and is powered by Google.

When you make Safe Search Kids your home page, or at the very least bookmark it for kids to

You May Like Sponsored Links



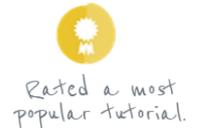
Abandoned Luxury Cars



- Home
- All Topics
- Internet Safety

Internet Safety

Phishing, trojans, spyware, trolls, and flame wars—oh my! If the idea of these threats lurking around online makes you nervous, then you can now be at ease. Our Internet Safety tutorial will provide you with the strategies, skills, and mindset needed to protect yourself, your computer, and your privacy when you connect to the Internet.



Visit our **Internet Safety for Kids** tutorial for lessons related to your children's safety.

Updated: February 19, 2015

 201  91  45  128

Internet Safety

1 Introduction to Internet Safety	2 Passwords: The First Step to Safety	3 Protecting Your Computer from Internet Threats	4 Email Tips for Scams and Spam	5 Staying Safe While Browsing
6 Protecting Your Financial Transactions	7 Smart Social Networking and Communication Tips	8 Cyberharassment, Stalking, and Addiction	9 Wireless and Mobile Device Safety	

Extras

Links to Resources for Internet Safety	I Have to Provide My Phone Number? Using Phone Verification	Quiz
--	---	------



- Home
- All Topics
- Internet Safety for Kids

Internet Safety for Kids

Practicing safety is a must with anyone who goes online, but with kids it is especially important. This tutorial will discuss the threats your kids may encounter while online, and it will show you how protect them and talk to them about being safe and responsible.

Visit our **Internet Safety** tutorial for more general safety practices that apply to everyone.

Updated: February 19, 2015



Internet Safety for Kids

- Teaching Kids About Internet Safety
- Staying Safe from Online Predators
- Cyberbullying and Cyberharassment
- Using Social Networks Safely
- Understanding File-Sharing Networks
- Mobile Device Safety
- Resources

Extras

- Five Free Ways to Protect Your Kids Online
- Quiz