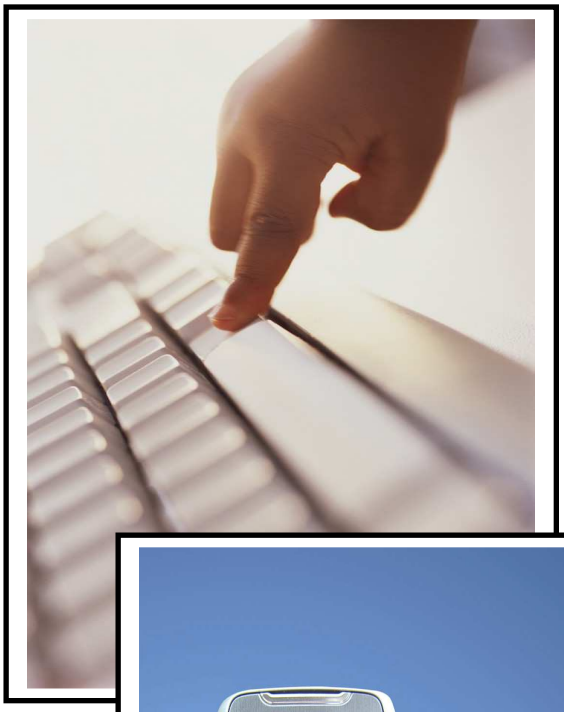
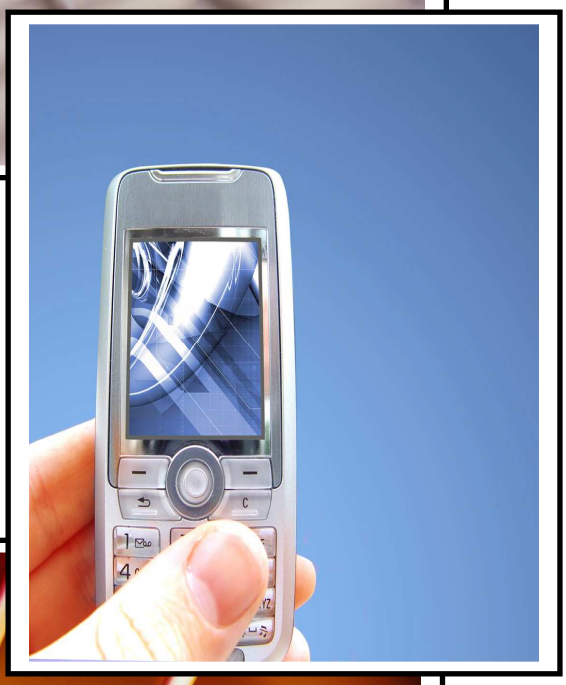
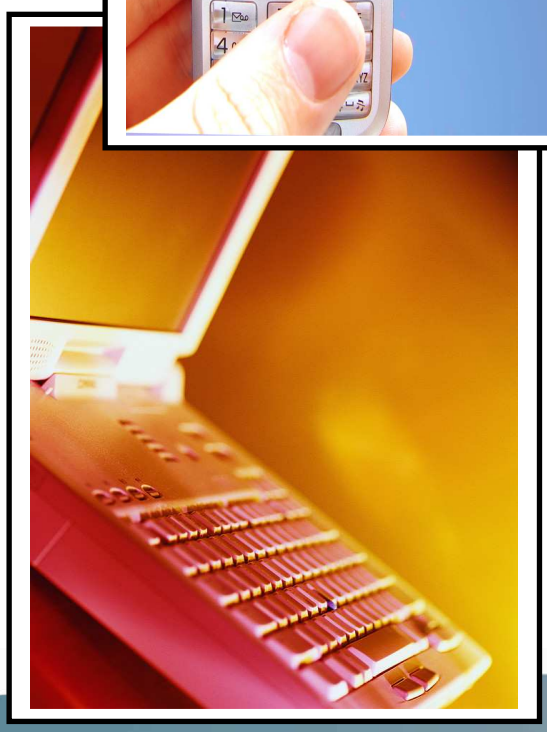






Responding to E-Safety

A Guide for Schools

Key Stage 1 & 2

Cardiff Against Bullying & the Cardiff Advisory Service for Education

Gwasanaeth Ymgynghorol Addysg Caerdydd
GYA CASE
Cardiff Advisory Service For Education

Cardiff Against Bullying • Caerdydd yn Erbyn Bwlio
cab

A Proud Capital

CARDIFF
CAERDYDD

Contents

Foreword

In recent years the face of education has changed many times over, and our pupils are now able to access a curriculum more rich and diverse than ever before, thanks in part to the wide range of technologies we can utilise as learning and teaching tools. The expanding rate of technological development affects every aspect of society, and the classroom has been enriched by the wealth of ICT resources now available to pupils and educators alike.

Whilst many of us have lived through the development of this technological revolution we see evident around us, enhancing our lives in many ways, it is clear that our children and young people only know a world where these technologies exist, and can little imagine a time without them. Our young people rely on the technology that is relatively new to us, not only utilising it as a method of learning, but to play, socialise, network and communicate with the world at large.

It is an exciting prospect to consider that our young people will be at the forefront of technological advances in the future, pushing the science of technology in directions we find difficult to envisage now. It is with this in mind that we come to consider how we will teach our pupils to use resources and tools that will undoubtedly be obsolete in a short space of time, to be replaced by faster, more advanced and complex technology.

Whilst we must strive to teach our young people how to use the tools, it is becoming increasingly evident that we must also focus on the safe and responsible use of technology – skills and awareness that will last a lifetime, no matter how the technologies change.

With increasing reports of abuses of technology, children engaging in risky behaviour, being subject to harassment or abuse and cyber bullying, it is clear that our role must be to promote e-safety within the ICT and PSE curriculum and adopting a whole school approach to e-safety to protect and educate our children about potential dangers.

It is with great satisfaction that we note the greater emphasis being placed on e-safety within the new ICT curriculum for Wales and the increased resources available to us from government agencies such as Becta. This resource, developed by Cardiff Against Bullying and the I.T. Advisory Service highlights once again how the city and county of Cardiff is at the forefront of promoting progressive, inclusive education for all its children and young people.

Chris Jones
Chief Schools Officer

The Importance of E-Safety

Statistics show us that more children and young people than ever before are now embracing new technology as a mode of communication, socialisation, recreation and learning. Technology such as the internet, email, mobile phones and games consoles are now a part of our society and a part of many of our daily lives. The benefits of such technologies are numerous and have changed and shaped the way in which we work, live and communicate with others. But as children of an increasingly younger age begin to use these technologies, there is a recognised need to educate and raise awareness with pupils of the risks, as well as the benefits, of new technologies. Becta, the government agency promoting the use of information and communications technology, state that e-safety education should begin as soon as technologies are introduced to children. Increasingly ICT is utilised throughout the curriculum, and certainly many children have access to the internet, games consoles and mobile phones at home. This presents a worrying reality – whilst we offer children the tools and teach them how to use them, are we also teaching responsibility, awareness and safety?

Whilst e-safety can be explored generally throughout the curriculum, whenever ICT is utilised as a learning and teaching tool, schools must also develop effective e-safety strategies, policies and specific education, for pupils of all ages. The implications of unsafe behaviour online or through the use of new technologies are substantial, and as such, the role of coordinating and embedding e-safe practices across the school should not fall solely to the ICT Coordinator or Network Manager, but rather should be adopted as a whole school approach, involving the whole school community, including parents and carers.

TEEN INTERNET USE

- Over half of 12-15 year olds have Instant Messenger (IM) conversations at least once a day and a third (33%) chat on IM several times a day
- 48% use email at least once a day

What is E-Safety?

E-safety relates to the education of using new technology responsibly and safely, focusing on raising awareness of the core messages of safe content, contact and commerce when using technology. This can include accessing websites and online content, email, online chat rooms, mobile phones, gaming and games consoles, social networking sites, instant messaging (IM) and viruses and spam.

There are a number of key risks to using new technologies, including:

- Physical danger
- Sexual abuse
- Bullying
- Identity theft
- Illegal behaviour
- Exposure to inappropriate content
- Obsessive use of ICT
- Copyright infringements

Safe content relates to keeping children from accessing or being exposed to inappropriate content, including that which is pornographic, hateful, violent, generally age-inappropriate or illegal. Safe content also relates to security risks such as adware, spyware, viruses and spam.

Safe contact relates to the risks associated with inappropriate contact through technology such as text messaging, online chat rooms, instant messenger (IM) and email. Risks include the danger of contact by paedophiles, the 'grooming' of children and young people, contact by people encouraging inappropriate or risky behaviour, for example meeting an online 'friend' in the real world, and cyber bullying, whereby technology is used to harass and bully. (See the cyber bullying section for more information).

Safe Commerce relates to the financial and commercial implications of using new technology, for example children giving out financial details online of a parent's credit card. Safe commerce also relates to registering with commercial websites safely, junk email and spam, premium rate services for mobile phones and awareness of online advertising and commercial advertising through other forms of new technology.

Why is E-Safety Important?

A study conducted by UK Children Go Online (UKCGO) from 2003-2005, of the use of the internet by children and young people aged 9-19, found that:

- 75% had access to the internet at home
- 92% had access to the internet at school
- 71% had access to the internet via a computer, with 38% gaining access via a mobile phone
- 38% of those surveyed trusted most information online
- 28% of parents who use the internet describe themselves as beginners compared with only 7% of children
- 79% of young people use the internet privately without their parent's supervision
- 57% of 9-19 yr olds have come into contact with online pornography accidentally
- 49% of children say that they have given out personal information, whilst only 5% of parents think their child had given out such information

Whilst many adults would consider themselves fairly proficient users of the internet and mobile phones, it is clear that children and young people now embrace technology in ways that older generations do not. The results of the survey by UKCGO are now three years out of date, and it is evident that young people's usage of technology is only increasing.

Whilst many of us used the internet to view information created by large corporations e.g. Microsoft, Amazon, BBC etc., in what was known as a 'web 1.0 environment', now users are increasingly favouring 'web 2.0' environments; as more people added their own content to the internet the environment began to change to become more interactive and personal. For example, now most newspaper homepages are not restricted to simply holding news articles, they interact with the user through offering videos, images, quizzes and user content. Today young people not only view content, they create it. Not only do they download content, such as music or images, but they upload it, adding their own views, music, images and so forth. Children and young people are now active participants in using and utilising new technology.

This demonstrates the importance of tackling and addressing e-safety, as young people's usage of technology changes and their skills become more proficient. Whilst most schools, libraries and public computers have filtering and monitoring software to negate any risky and inappropriate use, most home computers do not have the same safety features, and more importantly still, filtering or monitoring software does not teach children and young people what may be inappropriate to upload, how to deal with unwanted contact, the moral codes of conduct and rights and responsibilities. That role, as educators, is ours, in partnership with parents and carers, and children themselves.

The Role of Parents & Carers

Whilst the responsibility of teaching e-safety through the ICT curriculum may now lie with schools, there is a clear and important role for parents and carers to continue and reinforce the messages within the home.

With many parents stating their proficiency online and with new technologies as minimal, often the gap between children and parents can grow, leaving parents unsure about what their children are doing online and how to tackle it. Schools that wish to adopt a whole school approach to e-safety must recognise the importance of educating and assisting parents; a sample letter to parents introducing your e-safety policy is found in Appendix 1.

Whilst schools and council facilities will have filtering, monitoring and security software on computers to protect children from accessing inappropriate content, most home computers do not offer the same protection, and increasingly children and young people access the internet away from adult supervision – with computers in bedrooms or wireless internet access via mobile phones. There are also the moral and legal implications of children uploading content onto the web, sending inappropriate messages or images, engaging in cyber bullying and more, that needs continual education and reinforcement by parents and carers.

Surveys suggest that there is a widening gap between the online skills and proficiency of parents and their children, leaving many parents unsure of what their children are doing online and how to educate about safer and more appropriate use of technologies.

Schools can support parents and carers in this task by communicating school rules for e-safety and raising awareness of e-safety with parents through the promotion of policies, and specific presentations and sessions for parents highlighting the importance of the issue, promoting ways to make home technology safer.

Tips to help parents & carers

- Encouraging parents to put computers in family rooms (not in children's bedrooms) with the back of the computer against a wall
- Installing monitoring and filtering software to block access to inappropriate content (these types of software can be purchased from any IT store)
- Using a family email address, rather than children having their own private email addresses
- Discussing personal safety issues online with their children – e.g. not giving out personal information
- Become more internet-proficient – websites such as www.bbc.co.uk have information to help adults better understand the technologies

The Role of Parents & Carers

Parent & Carer Questionnaire

Included in this resource is a questionnaire for parents and carers (found in Appendix 2) that will allow schools to gain the views and perceptions of parents about both their use of the internet and other technologies, in addition to their perceptions of how their children use the internet.

Used in conjunction with the pupil questionnaire (found in lesson plan 1's resources) the results will allow schools to ascertain the differing uses of technologies by children and their parents and allow parents to ensure that they know what their children are doing online. Results of these questionnaires will also allow schools to develop e-safety lesson plans and schemes of work, based on the results gained, as well as target other work – awareness raising presentations to parents, for example.

Supporting Parents Further

CAB can provide presentations and sessions for parents and carers on e-safety and cyber bullying on request, providing an overview of the topics, tips and pointers for promoting e-safety at home and resources for parents to take away. Contact CAB at CAB@cardiff.gov.uk or on (029) 2061 7632 for more information.

To provide your own presentation to parents or for more information on supporting parents and carers with e-safety, visit:

www.childnet-int.org/kia

www.kidsmart.org.uk

www.thinkuknow.co.uk

www.ceop.gov.uk

E-Safety for Staff

Whilst education and awareness-raising about e-safety is crucial for pupils, it is also important that staff have an awareness of e-safety within their own classrooms or areas of work, including whilst using school equipment. Staff should be aware of the schools' policies and practices when using ICT as a teaching tool, researching and planning tool or when accessing private content in school, e.g. email. Schools need to make clear and appropriate guidelines for schools staff, for example outlining the appropriate use of school equipment such as a school mobile phone, digital cameras, computers, and the consequences of staff accessing inappropriate or unsuitable materials in school or engaging in illegal conduct through the use of school equipment.

A school E-Safety policy or ICT Acceptable Use policy is crucial to communicate these messages to staff and ensure staff awareness and understanding of new technology is consistent. Further guidance on creating or developing E-Safety or Acceptable Use policies is found in Section 6 of this resource.

The Roles & Responsibilities of Staff

Whilst e-safety is a whole school issue, there are differing roles for staff to assist in the development of a whole school approach. Class teachers and subject leaders should consider the implications of e-safety within their subject areas or within each lesson that utilises ICT as a teaching and learning tool, in addition to placing a specific focus on e-safety within ICT or PSE as a scheme of work.

Pastoral teams and senior management should consider the implications of responding to the welfare of pupils when there is an incident of ICT misuse or abuse, and the legislative framework when considering e-safety. This highlights the importance of a clear and accessible E-Safety or ICT Acceptable Use policy. It is also the role of senior management or the Head Teacher to coordinate and keep records of any misuse of ICT or abuses of technology that are reported to the school, and to inform relevant agencies as appropriate, such as the police.

The head teacher has the overall responsibility for e-safety and maintaining a safe ICT environment, and as such should coordinate, develop and promote policies to support staff in the awareness, development and delivery of e-safety. The head teacher should also act as the link to the Governing Body in ensuring they are informed and consulted on policy and curriculum changes and developments.

The head teacher, senior management or a network manager (should a school have one) is also responsible for maintaining ICT equipment, including its safe and responsible use by staff, ensuring that appropriate monitoring and filtering equipment is in place on school computers, and there are procedures to respond to the discovery of inappropriate use or content found on school equipment.

Creating an E-Safety Policy

Schools are encouraged to develop an e-safety policy to protect pupils and staff, and to ensure that the safety issues related to the use of technology are raised and considered by the whole school community. The report to the Welsh Assembly Government of the Schools ICT Strategy Working Group, 'Transforming Schools with ICT' states that "schools have a clear role to play in educating for and promoting the safe and responsible use of the Internet."

The purpose of an e-safety policy is to consider the safe use of the internet and other technologies within the school environment. The policy should establish the school rules and accepted use of technologies, how the school will protect pupils from the risks associated with the use of technology, and the role of the internet and other technologies in teaching and learning, including how pupils will be educated on e-safety specifically.

E-safety policies can encompass or sit alongside the ICT Acceptable Use policy, and should compliment and operate in conjunction with other school policies, such as the Child Protection policy, Behaviour policy and Anti-Bullying policy.

An e-safety policy should be regularly reviewed and updated – at least annually – to reflect the changes and advancements of technology.

Guidelines for Creating an E-Safety Policy

Considering the importance and risks associated with the use of the internet and other technologies by both pupils and staff, schools may wish to provide an e-safety coordinator to manage the implementation of the policy and monitor e-safety across the school. This may be the Head Teacher, member of the senior leadership team, ICT coordinator, child protection coordinator or network manager.

Schools may also wish to appoint a working party to develop the e-safety policy, and consult and gain the views of pupils (depending on their age), and parents and carers in the creation of the policy. The policy should be promoted to all staff across the school, in addition to parents and carers and should be approved by school governors.

The following points are guidelines for creating a school e-safety policy, and should be considered by each individual school for suitability and relevance.

Contents of an E-Safety Policy

Definition of e-safety

The policy should clearly state what e-safety is and why it is important for the school to consider. The definition should take into account the differing levels of competence and awareness of staff of new technologies, and as such the policy shouldn't use any acronyms without clear explanation, e.g. referring to instant messaging as IM.

Reference to other policies

The e-safety policy should reference and relate to other policies, including the child protection policy and anti-bullying policy. Schools should ensure that the contents of these policies are consistent, for example, sanctions for the misuse of technology are consistent and appropriate with sanctions for other poor behaviours.

Purpose of policy

A brief outline of the purpose of the e-safety policy – this should include the education, protection and awareness-raising of staff, as well as pupils.

The role of technologies within the school

The policy should outline which modes of technology are used in school and the accepted uses of the technologies, for staff and pupils. Consideration should be given to how the internet and other tools relate to teaching and learning, and how this will be managed by staff. Guidance for staff on the use of the internet and other technologies in and outside of the classroom (such as school mobile phones and digital cameras) should be outlined in the e-safety policy.

How e-safety will be taught

The policy should outline how and why e-safety will be taught to pupils, giving consideration to the age-appropriateness of teaching e-safety. The policy should outline who will coordinate the schemes of work for teaching e-safety- this may be the e-safety coordinator, should a school appoint one.

TEEN INTERNET USE

More than a quarter (27%) of teens use blogging services (online diaries) once a week or more, with one in 10 visiting blogs on a daily basis.

Contents of an E-Safety Policy

Managing internet access and technologies

The policy should give guidance on how the school will expect to manage the safety of pupils and staff when using the internet and other technologies.

Each aspect of technology should be separately headed, e.g. the internet, email, school website, social networking sites, and so on. The policy should reference the filtering and monitoring software that is in place, but should also encourage the reader to use their judgement when using the technologies. Rules for the use of technologies should be outlined in this section, e.g. Email – Pupils may only use school-system email accounts.

The misuse of technology

Linking to the behaviour and anti-bullying policies, the e-safety policy should reference the sanctions for pupils who misuse technologies or break the school rules with regard to e-safety. Sanctions should be consistent with those for other poor behaviours, for example a pupil using email or instant messaging to bully should be disciplined in accordance with the anti-bullying policy.

E-safety complaints

The policy should outline how complaints and reports of unsafe or risky behaviour are dealt with as guidance for staff – e.g. pupils inadvertently accessing inappropriate content online. Links should also be made with child protection procedures, should an issue of e-safety be a child protection concern. Pupils should be made aware of how to report incidents of technology misuse and cyber bullying and to whom. Young people can also report online abuse, including cyber bullying, via the Child Exploitation & Online Protection service (CEOP) at www.ceop.gov.uk.

Introducing the policy

The policy should outline how it will be communicated to staff and parents, and how the relevant contents will be communicated to pupils.

Staff roles and responsibilities

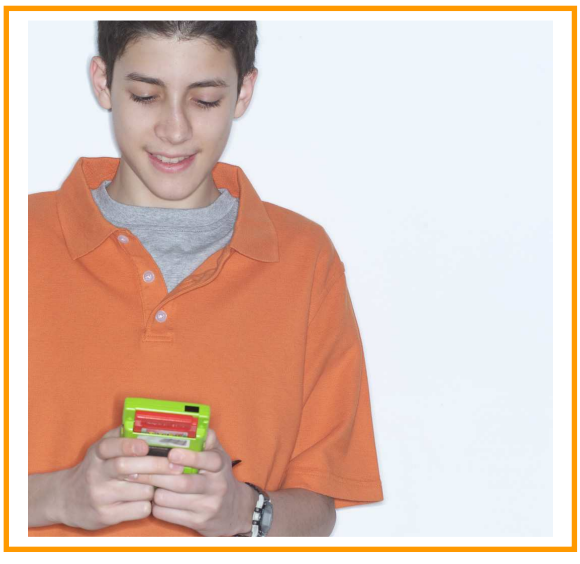
The responsibilities of all staff should be clearly outlined, including the responsibility of staff not to misuse technologies. Schools may wish to include a staff code of conduct for ICT to ensure all members are aware of their professional responsibilities when using ICT to communicate with and teach pupils.

Contents of an E-Safety Policy

Parent and carer responsibilities

Schools should consider how they plan to inform parents of the contents of the e-safety policy and whether they wish to gain parental permission for pupils to access the internet in school. Parents should also be made aware of the school rules for the use of the internet and other technologies, and encouraged to communicate these rules to children for the use of the internet and other technologies both in and outside of school. Policies should also outline the responsibilities of parents and carers in supporting the schools' message on e-safety.

Given the importance of parental understanding and support of e-safety, schools may wish to introduce the concept of e-safety to parents and carers through a parents evening or presentation.



Monitoring, evaluation and review

The policy should reference when and how it will be monitored and by whom, and provide a date for review.

How E-Safety relates to Curriculum 2008

As the onus on schools increases to provide education to use ICT safely, CAB and the IT Advisory Service recognise the importance of the delivery of specific e-safety lessons for pupils in key stages one and two, and have compiled a series of lesson plans and resources for primary and secondary schools, linking to the ICT, PSE and Citizenship curriculum.

The new ICT curriculum for 2008 now places a focus on teaching ICT safety and educating pupils of the hazards and risks of using technology. Appendix 4 contains an abbreviated abstract of the ICT curriculum for Key Stage 2.

The e-safety lesson plans and resources comply with the 2008 Programme of Study, notably, pupils will be learning to:

- Use ICT tools and suitable information safely and legally
- Use a range of ICT resources and equipment independently and collaboratively
- Become aware of new developments n ICT and consider the social, economic, ethical and moral issues raised by the impact and use of ICT

The scheme of work will place a focus on the health, safety and child protection guidance within the programme of study, and will consider:

- How and why we use new technology to communicate
- Risks and benefits of new technology
- Trusting and using online content
- Personal safety when using new technologies
- Irresponsible and unsafe behaviour
- Cyber bullying
- How to use equipment safely

E-safety and the legal framework

E-safety also relates to the legal use of the internet and other technologies by pupils and staff, as a number of aspects of use and abuse of the internet and other technologies are now governed by civil and criminal laws. Pupils and staff should be made aware of what activities could be deemed as criminal offences and how and when to report inappropriate or illegal acts, content or contact.

The following laws are relevant to the teaching and promotion of e-safety, but are not an exhaustive list. The impact and changing nature of the internet and other technologies suggests that changes to the law may occur, and as such professionals should inform themselves regularly and use their judgement when approaching e-safety.

- **Computer Misuse Act 1990**

(Including hacking, denial of service attacks, accessing files or software without permission).

- **Communications Act 2003 (section 127)**

(Sending a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, for example via the internet or mobile phone)

- **Sexual Offences Act 2003**

(Including grooming)

- **Data Protection Act 1998**

(Regarding the handling of personal information)

- **Malicious Communications Act 1998**

(Including harassment, bullying and cyber stalking)

- **The Obscene Publications Act 1959 and 1964**

(Including illegal material on or transmitted via the web and electronic communications)

- **The Telecommunications Act 1984**

(Including illegal material on or transmitted via the web and electronic communications)

More information and further details on these Acts and others can be found at www.opsi.gov.uk/acts

Cyber Bullying

A focus on cyber bullying in e-safety

Cyber bullying is defined as the use of technology (particularly mobile phones and the internet) to deliberately degrade, harass or hurt. As with traditional forms of bullying, cyber bullying can be intentional, repeated, and an imbalance of power can make it difficult for a victim to defend him or herself or seek help. Cyber bullying can occur in 7 main ways:

- By email
- Mobile Phone call
- Text message
- Instant Messenger (IM), e.g. MSN
- Online chat rooms
- Social Networking sites, e.g. Bebo, MySpace, Facebook
- Picture / video messages

Perpetrators will use these forms of technology to bully, for example posting harmful comments on a person's social networking profile. Cyber bullying can take many different forms, for example:

- **Threats and intimidation**
  Threats sent to people by mobile phone, email, or online, etc.
- **Harassment or stalking**
  Repeated, prolonged, unwanted contact or monitoring of another person.
- **Vilification / defamation / prejudice-based bullying**
  These may be general insults or racist, homophobic or sexist bullying.
- **Ostracising / peer rejection / exclusion**
  Set up of a closed group refusing to acknowledge one user on purpose.
- **Identity theft, unauthorised access and impersonation**
  'Hacking' by finding out or guessing a username and password.
- **Publicly posting, sending or forwarding information or images**
  Disclosing information on a website.
- **Manipulation**
  May involve getting people to act or talk in a provocative way.

TEEN INTERNET USE

In 2006 MSN (MSN.co.uk) produced a report into cyber bullying, based on a YouGov study of 518 children and their parents. The report found that:

In Wales:

- A quarter (25%) of young people know someone who's been cyber bullied
- 13% had experienced cyber bullying themselves
- 42% had endured cyber bullying for a week of longer
- Nearly two thirds (64%) had been cyber bullied by more than one person

SOURCE: MSN Cyber bullying report 06

Cyber Bullying

Cyber bullying can be an extension of face-to-face bullying, whereby a perpetrator uses the technology as an additional method to harass or upset their victim; however, cyber bullying does differ is a number of significant ways from more traditional forms of bullying:

- **24/7 contact** – traditional forms of bullying can be limited to the school yard or class room. The potential of cyber bullying is that it can constantly invade a person's home or personal space.

- **Impact** – there is the potential for cyber bullying to have a far wider and greater impact – with a potential worldwide audience, reached rapidly, and the possibility that the content will potentially stay online forever.

- **Perception of anonymity** – technological tools such as the internet and text messages gives a perception of anonymity that may encourage a young person to act in a way they wouldn't normally. There is less fear of being caught which can make the bullying more vicious and ferocious.

- **Profile of bully/victim** – cyber bullying changes the profile of the traditional 'bully' – anonymity can mean any person of any age, gender and size can feel able to bully another.

- **Bystander effect** – others can unintentionally contribute to cyber bullying and enhance the 'bystander effect', for example by forwarding on a humiliating message or image.

- **Evidence** – unlike with many traditional forms of bullying, cyber bullying offers inherent reporting proof in the form of message content, emails, images and so forth.

The legal implications

Whilst schools have a duty of care to protect pupils from bullying, there are additional legalities that impact upon preventing and responding to cyber bullying. The Education and Inspections Act 2006 (EIA 2006) states that Head Teachers had the power 'to such extent as is reasonable' to regulate the conduct of pupils when they are off site. Many incidents of cyber bullying take place beyond the school gates but impact upon pupils' well-being, academic ability and behaviour whilst in school.

Whilst cyber bullying is not a criminal offence, there are a number of laws which may apply, in particular for harassment or threatening behaviour:

- **Protection from Harassment Act 1997**
- **Communications Act 2003**
- **Malicious Communications Act 1988**
- **Public Order Act 1986**
- **Obscene Publications Act 1959**

As cyber bullying can appear to be an anonymous act, it is important to inform pupils of the legal implications and consequences of such behaviour.

Cyber Bullying

Preventing Cyber Bullying

Cyber bullying relates clearly to e-safety education, as the importance of equipping young people with rights, responsibilities and self-regulation when using technology also extends to acknowledging the way in which the technology is used in relation to others. Educating pupils to understand what cyber bullying is, its impact, and how to respond to it should be embedded within the wider e-safety curriculum.

Technologies such as mobile phones and the internet are a huge part of young people's lives, and whilst their use may be restricted in schools it is important to recognise that many children and young people have free and often unrestricted use of these technologies outside of school. Therefore the need to educate and inform pupils of how to use technology responsibly is crucial.

There are a number of ways in which to prevent cyber bullying:

- **Policy:** the school's anti-bullying policy should reference cyber bullying as a discreet form of bullying, providing a definition and acknowledging the ways in which the school will respond. A schools' ICT Acceptable Use policy and/or E-Safety policy should also reference cyber bullying.

- **Awareness Raising:** including through specific e-safety lessons with pupils, consideration should be given to promoting awareness and understanding of cyber bullying, including equipping pupils with the understanding to respond effectively to incidents of cyber bullying, and recognising positive and safe uses of technology.

- **Promoting Awareness with Parents:** as cyber bullying will often occur outside of school it is important that parents and carers are made aware of what cyber bullying is, how it can be prevented in the home and how they can respond to incidents.

TEEN INTERNET USE

Girls are:

- Twice as likely to know someone or several people who have been cyber bullied - over a third (34%) compared to one in six boys (17%)
- More likely than boys to have been victims of cyber bullying themselves (18%)
- More likely than boys to think cyber bullying is worse than physical bullying (14%)

SOURCE: MSN Cyber bullying report 06

Cyber Bullying

Responding to Cyber Bullying

Incidents of cyber bullying should be dealt with by the school in the same manner as any other form of bullying, with incidents recorded, investigated and support offered for victims, and sanctions for perpetrators provided in accordance with the schools' behaviour and anti-bullying policies.

A pupil who has experienced cyber bullying should be encouraged to not retaliate to messages or comments made, to take steps to block bullies from contacts lists (e.g. on their social networking site or instant messaging contacts list), to change passwords or their mobile phone number, and to save any content as evidence. Pupils should also be provided with ways in which to report incidents of cyber bullying, for example contact numbers for Internet Service Providers or mobile phone providers, many of which now employ specific malicious calls teams. Pupils and their families should also be advised when an incident may be a police matter.

Schools should also be aware that staff can also be victims of cyber bullying, and this should be reflected within anti-bullying policies and similar. Staff should be made aware of what cyber bullying is and how they can respond to it.

CYBER BULLYING FACTS

- **1 in 20 teens admit to being involved in bullying someone else online.**
  SOURCE: MSN Cyber bullying report 06

Further guidance

There are a number of useful resources available to support schools in addressing cyber bullying. Guidance has been produced by the DCSF entitled, 'Safe to Learn: Embedding Anti-Bullying Work in Schools' which can be accessed at www.teachernet.gov.uk/publications

CAB can also provide direct support to schools and other services on cyber bullying on request.

Cyber bullying & the lesson plans

The e-safety scheme of work produced by CAB and the IT Advisory Service addresses the issue of cyber bullying for Key Stage 2 and 3 pupils, recognising the incidents of cyber bullying and misuse of technologies that have taken place by children as young as 7 or 8. The aim of the lesson plans and resources are to offer opportunities for highlighting the risks as well as benefits of the technologies, encouraging safer, more responsible use.

Appendices

Appendix	Title
1	Sample letter to parents and carers
2	Parent & Carer Questionnaire
3	ICT Curriculum 2008
4	E-Safety Lesson Plans and Resources
5	Bibliography

Dear Parent / Carer, 20th September 2009

Re. xxxx Primary School's E-Safety policy

Xxxx Primary School has recently created an e-safety policy for staff, pupils and parents. We recognise that the internet and other technologies can be teaching and learning tools and enhance the curriculum and skills of pupils, but there are recognised risks associated with being online and using other forms of technology, such as mobile phones.

Therefore, xxxx Primary School will now be teaching e-safety to pupils as a part of the ICT and Personal Social Education (PSE) curriculum. These lessons will focus on equipping children with the skills and understanding how to be safe online, including:

- The risks and benefits of technology
- Making appropriate judgements about online content
- Personal safety online
- Using equipment safely and being responsible online

I would like to take this opportunity to share with you our school rules for the safe use of the internet and other technologies, a copy of which are enclosed.

Copies of our new e-safety policy can be obtained on request from the school office.

Yours sincerely,

Name
Head Teacher

……

Permission for internet access
Parent / Carer's Consent

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

Signed: _____

Print name: _____

Date: _____

Pupil Agreement

I agree to follow the rules for e-safety

Signed: _____

Print name: _____

Class: _____

Parent / Carer E-Safety Questionnaire

Please complete the following information by ticking the appropriate boxes. Thank you.

Number of children …… **Boy** ◯

Age/s:…….. **Girl** ◯

1.) Does your child have the following: *(please tick as many options as you wish)*

Mobile phone ◯ Home computer ◯ Laptop ◯ Games console ◯ MP3 music player ◯

2.) How does your child access the internet? *(please tick as many options as you wish)*

In school ◯ Home computer ◯ Mobile phone ◯ Through TV ◯ Through a games console ◯

3.) If you have a computer at home, where does your child use it?

In their bedroom ◯ In a family room ◯ In a home office ◯ Portable – e.g. laptop ◯ Other ◯

4.) How often does your child use the internet?

Every day ◯ More than once a week ◯ Once a week ◯ Once a month ◯ Less than once a month ◯

5.) If your child uses it every day, how many hours do they use it for?

Less than 1 hour a day ◯ 1 – 2 hours ◯ 2 – 3 hours ◯ 3 – 4 hours ◯ More than 4 hours a day ◯

6.) What does your child like doing the **most** online? *(please tick as many options as you wish)*

Chat Rooms ◯ Blogs (online diary) ◯ Music (e.g. iTunes) ◯ News ◯

Instant Messenger (MSN, Yahoo) ◯ Gaming ◯ File sharing (e.g. Limewire) ◯ Internet TV ◯

Social Networking (Bebo, Myspace) ◯ Web Browsing ◯ Shopping ◯ Other (Please specify)

……

7.) How often do **you** use the internet**?**

Every day ◯ More than once a week ◯ Once a week ◯ Once a month ◯ Less than once a month ◯

8.) What do **you** like doing the most online? *(please tick as many options as you wish)*

Chat Rooms ◯ Blogs (online diary) ◯ Music (e.g. iTunes) ◯ News ◯

Instant Messenger (MSN, Yahoo) ◯ Gaming ◯ File sharing (e.g. Limewire) ◯ Internet TV ◯

Social Networking (Bebo, Myspace) ◯ Web Browsing ◯ Shopping ◯ Email ◯

9.) Does your child use **social networking** sites like Bebo and Myspace?

Yes ◯ No ◯ Don't know ◯

10.) If you have a home computer or laptop, does it have **filtering and/or monitoring software**? (e.g.
software that blocks children accessing some websites and content)

Yes ◯ No ◯ Don't know ◯

11.) How would you describe your online skills?

No skills at all ◯ Beginner ◯ Average ◯ Adept ◯ Expert ◯

12.) Has your child ever received an unwanted or upsetting text message or email?

Yes ◯ No ◯ Don't know ◯

Cardiff Against Bullying • Caerdydd yn Erbyn Bwlio
cab

13.) Has your child ever accessed inappropriate content online, e.g. adult content?

Yes ◯ No ◯ Don't know ◯

14.) Has your child ever given out personal information online? (e.g. address, phone number)

Yes ◯ No ◯ Don't know ◯

15.) Has your child ever been the victim of cyber bullying (when technology such as text messages, email or websites are used to bully)?

Yes ◯ No ◯ Don't know ◯

16.) How concerned are you about your child's safety online and when using technology such as mobile phones?

Very ◯ A little ◯ Not at all ◯

17.) Would you like more help, support and information about e-safety?

Yes ◯ No ◯

Thank you for completing this questionnaire.
Your answers will allow CAB and your child's school to teach children to use the internet and other technologies safely and better support parents and carers.

Please return your completed questionnaire to your child's school.

Cardiff Against Bullying (CAB)
CAB@cardiff.gov.uk

Key Stage 2 Programme of Study

Skills

Find and analyse information

Pupils should be given opportunities to:

1. discuss the purpose of their tasks, the intended audiences and the resources needed
2. find information from a variety of sources for a defined purpose
3. select suitable information and make simple judgements about sources of information
4. produce and use databases to ask and answer questions, *e.g. search, sort and graph*
5. produce and use models and/or simulations to ask and answer questions, *e.g. use a spreadsheet to calculate and graph sales in a shop*
6. investigate the effect of changing variables in models and/or simulations to ask and answer 'what if…?' type questions.

Range

Pupils should be given opportunities to:

- use ICT tools and suitable information sources safely and legally, in accordance with LEA/school guidelines
- use a range of ICT resources and equipment independently and collaboratively, *e.g. cameras, scanners, CD/DVD players, MP3 players, mobile phones, PDAs*
- use ICT sources of information and non-ICT sources of information
- use ICT to further their understanding of information they have retrieved and processed
- use ICT to explore and to solve problems in the context of work across a variety of subjects
- draw upon their experiences of using ICT to form judgements about its value in supporting their work
- store and retrieve information they have found or created
- evaluate their work and learning
- discuss new developments in ICT and the use of ICT in the wider world.

Create and communicate information

Pupils should be given opportunities to:

1. create and communicate information in the form of text, images and sound, using a range of ICT hardware and software
2. create a range of presentations combining a variety of information and media, *e.g. a poster combining text and graphics, a multimedia presentation*
3. share and exchange information safely through electronic means, *e.g. use of e-mail, virtual learning environments.*

Health, safety and child protection

Pupils should be taught how to use ICT comfortably, safely and responsibly, and to consider the hazards and risks in their activities, *e.g. the importance of not disclosing personal details to strangers*. They should be able to follow instructions to minimise risk to themselves and others.

The full ICT curriculum can be found at www.wales.gov.uk

Key Stage 2 Lesson Plans

Contained within this resource are e-safety lesson plans and resources for Key Stage 2 pupils.

These lessons explore the key aspects of e-safety including how and why we communicate, methods of communication, sharing information using new technologies, trusting online information, keeping personal information private and cyber bullying.

The lesson plans contain all resources and supplementary information needed, and can be used as a scheme of work in its entirety, or can be adapted as necessary to meet the needs of your pupils.

Each plan builds upon the previous lesson, developing knowledge and understanding in pupils, but each lesson can be used in isolation.

The aims of each lesson are:

1. How and why we communicate
2. Keeping personal information private
3. Staying safe online
4. Trusting content
5. Chatting safely online
6. Cyber bullying

There are many additional resources and lesson plans to supplement and build upon this scheme of work. A good site for teacher resources has been developed by CEOPS (the Child Exploitation and Online Protection Centre) which can be found at www.thinkuknow.co.uk

This website also includes downloadable assemblies, films and questionnaires and you can also order free resources to be sent to your school such as pupil leaflets and posters and parent/carer leaflets in both English and Welsh.

Whilst the individual lessons can be delivered in isolation, as a part of Anti Bullying Week awareness-raising for example, CAB and the IT Advisory Service stress the importance of placing an emphasis on e-safety throughout the school year and developing or returning to a scheme of work year on year, in addition to raising the issue of e-safety in regular assemblies, through PSHE or circle time sessions, when anti-bullying is discussed, during Safer Internet Day in February each year and whenever ICT is utilised as a learning and teaching tool.

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: **Communicating With Others**

Duration: 1 hour **Lesson:** 1 **Key Stage 2**

Lesson Aim: To investigate how and why we communicate with others, exploring the risks and benefits.

Learning objectives:	**Resources:**
• To explore and identify methods of communication. • To understand why people communicate. • To understand the risks and benefits of various modes of communication.	Pupil Questionnaire (Think U Know) Pupil Worksheet – 'How We Communicate' Different forms of communication for pupils to review – letter, fax, leaflet, poster, email, etc. **Vocabulary:** Communication, e-safety, technology, internet, risk, benefit, personal, private.

Introduction: 15 mins

Introduce the topic of e-safety – what it means and why we need to be aware of our safety when using different technologies.

Activity 1: Pupil Questionnaire 15 mins

Using Resource 1 – the pupil questionnaire, ask each pupil to complete the questionnaire to explore how they use new technologies. You may wish to go through each question with the whole class group for those pupils who may not understand some of the terminologies. Stress that answers should be kept private and that the results will be confidential.

The results of the pupil questionnaire when collated will allow you to judge the knowledge and expertise of your pupils in using new technologies, and if they are engaging in potentially risky activities. This will allow you to further direct lesson delivery and highlight the need for more intensive work, including with parents and carers, should there be a need.

Activity 2: How we Communicate 15 mins

Ask pupils to list different methods of communication and write them on the board. Discuss which are traditional forms of communication and which are newer. E.g. letter, email, phone call, fax, etc.

In groups, ask pupils to discuss which methods of communication they would use for a variety of situations, using **Resource 2 – 'How We Communicate' pupil worksheet**.

Ask pupils to feedback their results and discuss as a class.

Discussion Points:

Which methods of communication do we use most?
Do our friends use the same methods of communication? Do our parents?
Is there a difference between how children and young people communicate, and how older people and adults communicate? Why?
Are some forms of communication more appropriate for some purposes?

Activity 3: Risks & Benefits 15 mins

As a class, list the risks and benefits of the different forms of communication.

Discussion Points:

Are some forms of communication more risky than others? (E.g. internet chatting over a telephone call or letter?)
What do these risks mean for us when we're using these methods of communication?
Should the risks stop us using some forms of communication?

Conclusion 5 mins

Recap on the main points discussed – who we communicate with, why and how, and the risks and benefits of forms of communication.

Discussion Points:

Have you learnt anything about who we communicate with and how?
Is there anything you would change in the future when you're communicating with someone you can't see (e.g. online chatting, text message)?

Opportunity for assessment: Most pupils should be able to:

- Name a number of forms of traditional and new methods of communication.
- Identify risks and benefits of forms of communication.
- Understand the concept of personal and private information.
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

You will need to ensure that the class consider new forms of technology as tools for communication, such as:

- Online chatting
- Text message
- Picture message
- Websites
- Social Networking sites (e.g. MySpace, Bebo, Facebook)
- Phone call
- Blogs or Vlogs (online diaries or online video diaries)

Encourage pupils to consider why more young people are using these forms of communication than older people. You may wish to highlight that until very recently most people only communicated face to face or in a delayed fashion, such as through letter-writing. Now communication is instantaneous. Are there any benefits and risks to instant communication?

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: Personal Information

Duration: 1.5 hours **Lesson:** 2 **Key Stage 2**

Lesson Aim: To explore how to be safe online and the importance of keeping personal information private.

Learning objectives:	**Resources:**
• To explore the ways in which pupils communicate • To understand the concept of personal and private information. • To understand safety rules and responsible behaviour when using new technologies. • To explore how and why we share information, give information and receive information. • To understand the concept of personal safety in real life and 'online life'.	Pupil Questionnaire results Pupil worksheet 3 – 'Who Would You Tell?' (Different forms of communication – spam email, leaflet, junk mail, etc) **Vocabulary:** Communication, e-safety, technology, internet, risk, benefit, personal, private.

Introduction: 5 mins

Recap on the previous lesson content – how we communicate, with whom and why. Recap on some of the risks and benefits of different forms of communication, including traditional and newer forms. Explore if newer forms of communication are more risky and hold additional dangers we should be aware of, and why this may be, (e.g. chatting online may hold additional risks than chatting with someone in person because they may not be who they say they are).

Activity 1: Pupil Questionnaire Results 10 mins

Using the collated results of the pupil questionnaire, feedback to pupils what the main forms of communication are for pupils in the class. Discuss if the results surprise them or were expected.

Discussion Points:

Do all children have access to the forms of communication we do, (such as mobile phones and the internet)?
Did children always communicate in these ways?
How have we learnt to use these forms of communication?
Has anyone ever discussed the risks or safety issues with these forms of communication?

Activity 2: Asking, giving, sharing information 30 mins

Discuss and list the reasons **why** we communicate with others. Highlight the difference between forms of communication that are **asking** for information, **giving**

information and **sharing** information.

If possible, display a number of forms of communication for pupils to review and decide whether they are risky or of benefit, and what makes them risky or beneficial – e.g. a letter from a friend, junk mail, an example of a spam email, a poster advertising something, a leaflet, etc.

In groups, ask pupils to complete the **'Who would you tell?' worksheet – Resource 3**. This worksheet provides examples of a number of pieces of information that could be revealed, asking pupils to consider who they would tell the information to.

Discuss the concept of personal and private information.

Discussion Points:

What would you need to consider before deciding something is risky or of benefit (i.e. who has written it, the contents, whether its asking for something, if you trust the contents or author, etc).
What information would you be happy to give to anyone?
What information would you like to keep private? Why?
Do we also need to consider what information we're asking others for, as well as the information we're giving to others?
Are there some people we wouldn't want to communicate with at all?
How would we know who these people were if we were chatting online?

Activity 2: Personal Safety in Real Life **15 mins**

As a class, discuss how pupils would make sure they were safe in day to day life. What would they do to maintain their safety? E.g. when crossing the road, using dangerous objects such as scissors or knives, not talking to strangers. Discuss what makes them think about their safety – e.g. they know something is dangerous, they don't trust someone, they feel frightened. Discuss if these rules apply when online or communicating with someone you can't see.

Activity 3: Giving out Personal Information **15 mins**

Recap on the earlier discussion about who we would give information to that is personal to us, and when we have to be careful about giving out personal information.

This simple guessing game will encourage pupils to further consider how personal information can be used to identify someone. Ask pupils to work in pairs or play as a whole class. The teacher or one pupil in the pair gives a description of a person they are thinking of, either a person in the school or a celebrity most of the children will know. Pupils have to guess who is being described, e.g.

"I'm thinking of a girl in year 5 with blonde hair…."
"I'm thinking of a very famous person who plays football…"
"I'm thinking of a teacher whose name begins with an S…."

Pupils may ask questions to gain further clues before identifying the person.

Discussion Points:

What information helped you to identify the person you were thinking of? Sometimes we only need one or two pieces of information to identify someone, sometimes we need more to piece together.
Do we need to think about the information we're giving to people about us? Why?

Conclusion **5 mins**

Recap on the main points discussed – what is personal information, how we would keep ourselves safe in real life, why we need to keep safe when online or chatting with those we don't know, how we identify people using personal information and what to consider when chatting online and using new technologies.

Opportunity for assessment: Most pupils should be able to:

- Name a number of forms of traditional and new methods of communication.
- Identify risks and benefits of forms of communication.
- Understand the concept of personal and private information.
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

If possible, log in to an internet chat room and observe general conversation, or visit the chat room element of the CEOPS/ThinkUKnow Cyber Café (the Cyber Café is a teaching and learning resource designed for children, focusing on teaching internet safety, and will be utilised within these lesson plans). There is a chat room element within the Cyber Café that demonstrates how internet chat works.

Chatting online can breed almost instant familiarity and it's very easy to feel at ease and comfortable to share information in a chat facility that a person wouldn't necessarily share face to face. You should be aware of how easy it is to illicit and provide personal information when chatting, to truly impress upon pupils the need to be consciously aware of their actions when online.

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: **Staying Safe Online**

Duration: 1.5 hours **Lesson:** 3 **Key Stage 2**

Lesson Aim: To explore how to be safe online and the importance of keeping personal information private.

Learning objectives:

- To understand the concept of personal and private information.
- To understand safety rules and responsible behaviour when using new technologies.
- To understand the concept of personal safety in real life and 'online life'.
- To learn the SMART rules for when using the internet.
- To explore the difference in communicating face-to-face and online.

Resources:

'Personal!' cards and question prompts
Resource 4 – SMART Thinking
Resource 5 – Statements & Scenarios (you will need a copy per group)

Vocabulary: Communication, e-safety, technology, internet, risk, benefit, personal, private, SMART.

Introduction: 5 mins

Recap on the previous lesson content – different forms of communication can be asking for information from us, we can be sharing information or giving information. Some information is personal and should not be shared. Giving out personal information to others can provide them with clues as to who we are that we might not necessarily want them to know. We sometimes give out personal information to others that should remain private.

Activity 1: Personal! 15 mins

Group pupils into 3's to play the Personal! game, giving one person in each three a Personal card. One pupil should ask another a series of questions about them, as if they were chatting having never met each other before. If it is safe to do so, the pupil can respond, but if their answer requires some personal information they must hold up the Personal card. The third person should observe and note any time that personal information was given without the person realising, feeding back at the end of the game.

Discussion Points:

Did anyone give away any personal information by mistake?
How easy was it to try and make someone give some personal information?
Discuss the need to keep information private when chatting online or with someone we don't know, as they may not be who they say they are, or we're not sure we can trust them.
Discuss the thought that some people may feel they are being rude by not responding to someone's questions about their age or where they live, but that they wouldn't give out such information to someone they didn't know on the street.

Activity 2: SMART 10 mins

Introduce the SMART message – see **Resource 4 – SMART thinking**, and discuss why the SMART message is so important.

(As an extension activity you may wish to ask pupils to create a SMART thinking poster to display near the classroom computer or in the ICT suite).

Activity 3: Statements and Scenarios 25 mins

Pupils should work in small groups. Give each group a pair of scissors, and a copy of **Statements and Scenarios**. As a whole class or within their groups, ask pupils to look at the statements and scenarios and then cut them into strips. Ask pupils to decide whether each statement/scenario describes a face-to-face interaction, or an online communication, or if any apply to both.

As a class look at each of the statements/scenarios and where each group has placed them. Did everyone agree? Ask pupils if anyone has experienced one of these scenarios and would be willing to share. Explore if pupils had considered before that some things are only suitable for face-to-face interaction, and why. Does this change the way they might conduct themselves when online now?

Conclusion 5 mins

Recap on the main points discussed – what is personal information, why shouldn't we give out our personal information to people, what are the SMART rules and the differences in communicating online to communicating face-to-face.

Opportunity for assessment: Most pupils should be able to:

- Understand the concept of personal and private information.
- Understand and relay the SMART rules
- Understand the difference between communicating online and face-to-face, and some of the dangers associated in communicating online.
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

When discussing online and face-to-face communications, teachers should be willing to discuss some of the dangers or pitfalls associated with online communication, (e.g. if you don't know who you're talking to online, why this could be dangerous). However, it is important to provide a clear and healthy balance between making children aware of the dangers, whilst also placing an emphasis on the many benefits of new technologies – including chatting online. Teachers should avoid sensationalising the issue, whilst ensuring children are made aware.

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: **Trusting Content**

Duration: 1.5 hours **Lesson:** 4 **Key Stage 2**

Lesson Aim: To explore online content, making judgements about the trustworthiness and suitability of websites.

Learning objectives:	**Resources:**
• To explore the validity of information on the internet • To begin to make sensible and considered judgments about whether or not to trust online content • To compare and contrast different sources of information. • To explore the difference in communicating face-to-face and online.	Resource 6 – Trusting Content: Quiz Questions Resource 7 – Quiz worksheet Resource 8 – Comparing Websites worksheet **Vocabulary:** Communication, e-safety, technology, internet, risk, benefit, personal, private, SMART, website, web address, search engine, search bar, trust, compare, user-friendly.

Introduction: 5 mins

Recap on the previous lesson content – what is personal information, why shouldn't we give out our personal information to people, what are the SMART rules, and what are the differences in communicating online to communicating face-to-face.

Activity 1: Exploring the Internet 15 mins

As a whole class, discuss the different types of information that is published on the internet, making a list on the board. Ask pupils how information on the internet is different from that in books, newspapers, magazines or television. Is it necessarily more accurate and up to date? Why do we use it? What are the advantages?
Ask pupils if there are any disadvantages or risks associated with using information on the internet.

Activity 2: Trusting Content 25 mins (You will need to ensure each child or pair/small group has access to a computer with the internet.)

As a class, discuss how you would search for something on the internet (i.e. using a search engine.) If you have a preferred search engine in school, draw the children's attention to this as they will be searching for answers to questions in a special quiz. If you don't use a specific search engine, try Google www.google.co.uk or for a child-specific engine (where access to sensitive material is limited) try www.askkids.com

Show children how you search for information, using the search bar, for those who don't know.

Using **Resource 6 – 'Trusting Content: Quiz Questions'** ask children to work in pairs

or small groups to find answers to each of the questions as quickly as possible, recording their answers on the **quiz worksheet – Resource 7**. They will need to record their answer, where they found the information (the website address) and which search engine used. You may wish to do question 1 as a whole class to assist those children who may struggle with searching online.

Discussion Points:

Compare answers across the class – did we all get the same answer?
Did we all use the same websites to find the answers? If not, why? (Discuss the vast number of websites that contain the same information)
How do we know if a website is telling the truth?
What could this mean, when we're searching for important answers or information? (I.e. that we shouldn't trust everything we read and see, and should look to 'back it up' – finding more than one source to prove the answer is right.
Do we trust everything that is on the internet? Why not?
What is it about a website that makes us trust the information? (Who it's made by – e.g. BBC, what it looks like, how easy it is to find our way around, etc).

Activity 3: Comparing Websites 15 mins

Ask pupils to choose two different websites from the following list to explore, spending time browsing the content and getting a feel for the site. Ask pupils to them complete **Resource 8 – Comparing Websites worksheet**. The worksheet asks them to evaluate the site, considering:

- Is it attractive and user friendly?
- Does it contain anything that makes them feel uncomfortable?
- Do the headings look relevant for what they want to find out?
- Are the links useful?

www.cbbc.co.uk
www.
www.
www.

Discuss what we should do if we don't trust a website. What should pupils do if they feel uncomfortable with what they see on a website?

Conclusion 5 mins

Recap on the main points discussed – we can't always trust the information we find on the internet. We must use our judgement when deciding what we believe from what we read on the internet. It is important to tell someone if we feel uncomfortable with something we see on a website.

Opportunity for assessment: Most pupils should be able to:

- Understand the difference between online content and more traditional forms.

- Make judgments about the validity and suitability of websites
- Consider whether they trust the content of websites
- Understand and relay the SMART rules
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: **Chatting Online**

Duration: 1.5 hours **Lesson:** 5 **Key Stage 2**

Lesson Aim: To explore how to chat safely online.

Learning objectives:

- To understand how to use chat rooms sensibly and safely.
- To begin to make sensible and considered judgments about whether or not to trust online content and people when online
- To compare and contrast different sources of information.
- To explore the difference in communicating face-to-face and online.

Resources:

Resource 9 – Case Study
Resource 10 – Case Study Worksheet
Access to the internet

Vocabulary: Communication, e-safety, technology, internet, risk, benefit, personal, private, SMART, website, web address, chatroom, Instant Messenger.

Introduction: 5 mins

Recap on the previous lesson content – what we should look for when deciding if we trust a website, what to do if we don't trust a website or it makes us feel uncomfortable; we can't always trust the information we find on the internet. We must use our judgement when deciding what we believe when we read information on the internet.

Activity 1: Why Chat? 15 mins

Refer back to the questionnaire results or ask pupils to raise their hands if they chat online. Discuss how regularly pupils chat, and to whom. Do pupils chat to friends in real life? Who else do we talk to? Typically, how many contacts do we have on our friends-lists?

Discuss which methods pupils generally use to chat (e.g. MSN [Instant Messaging], specific chat sites or gaming sites with chat facilities.) Discuss why people chat online. What are the benefits? Risks?

Activity 2: Case Study 15 mins

Using **Resource 9 – Case Study – Chatting online**, read the case study aloud to the class. Ask pupils to work in small groups to complete accompanying **Worksheet - Resource 10**, asking pupils to consider:

What information should Abby **not** have revealed?
Why do you think Abby gave that information?
Why is it not a good idea for Abby to have given that information?
What could Abby have done instead?
What could she do now?

Who can Abby tell if she is worried or upset?

As a whole class, share answers and explore any similarities and differences in answers.

Activity 3: Cyber Café 25 mins *(For this activity, all pupils will need to have sight of a computer with internet access, working individually, in pairs or threes).*

Pupils will be exploring how to chat at the Cyber Café – a Think u Know resource. Teachers are urged to explore the site before asking pupils to do so. The Think u Know website has a number of useful resources for children, teachers and parents. Visit www.thinkuknow.co.uk for more information.

The Cyber Café is a young person's resource to safely explore aspects of the new technologies such as chatting online, email, mobile phones. It is an interactive, animated resource designed to educate children whilst having fun.

Ask pupils to type http://www.thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx or click on Cyber Café from the Think u Know main site. Ask pupils to scroll across to the left and click on the character 'Sam'. This will take you to the section of the Cyber Café exploring chat rooms. The character Sam is chatting in a chat room. The site asks pupils to choose a chat room The site will take users through Sam's conversation with other children in the chat room. They are then asked to make decisions on Sam's behalf about who he should talk to and what information he should give out to other chatters. Users can click on the 'Chat room help' button on the right hand side at any time if they are stuck. With each answer, advice and pointers are given to the user.

As a class, discuss how realistic the chat room was, relating it to their experiences of chat rooms. Discuss how useful the advice given was and if they would use or have used a moderated chat room especially designed for children. Why?

Activity 4: Chatting Online, Chatting in Real Life 15 mins

Draw three columns on the board entitled, 'Chatting in Real Life', 'Chat room' and 'Instant Messenger Chat'. Discuss the differences between the three, noting down in each column what you would need to consider to keep yourself safe when involved in each type of 'chat'. Discuss what the similarities and differences are in these 3 forms of chat.

Activity 5: Chatting Rules! 10 mins

Discuss if the same rules apply when chatting online as chatting in real life? (E.g. good manners, speaking nicely, being safe, not giving out personal information, etc). Are there any extra rules? Using the information gathered in the columns, create a few simple rules to remember when chatting online, referring back to the SMART rules also. You may wish to display these near to computers and in the ICT suite.

Conclusion 5 mins

Recap on the main points discussed – chatting online and chatting in person is different, but the same rules apply. We need to be extra careful when chatting online.

Opportunity for assessment: Most pupils should be able to:

- Understand what online chatting is and navigate their way around a chat room
- Identify a number of rules that apply to online chatting.
- Identify the difference between online chatting and chatting with someone in the real world.
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

SCHOOLS & LIFELONG LEARNING SERVICE

Cardiff Against Bullying - Lesson Plans

Title: E-Safety: **Cyber Bullying**

Duration: 1 hour **Lesson:** 6 **Key Stage 2**

Lesson Aim: To understand and define cyber bullying, exploring how to combat it.

Learning objectives:	**Resources:**
• To define cyber bullying • To explore the differences and similarities between cyber bullying and more traditional forms of bullying • To identify different forms of cyber bullying • To understand what to do if confronted with cyber bullying	Resource 11 – Similarities & Differences worksheet **Vocabulary:** Communication, e-safety, technology, internet, risk, benefit, personal, private, SMART, website, web address, chatroom, Instant Messenger, text message, cyber bullying, bullying, definition.

Introduction: 5 mins

Recap on the previous lesson content – when chatting online we need to be aware of different rules and our safety. Chatting online is different from chatting in person. Some conversations are more appropriate for face-to-face.

Activity 1: What is cyber bullying? 15 mins

As a class, brainstorm what bullying is, and what types and forms it can take. Discuss where bullying may take place and when, drawing on pupils' experiences of witnessing bullying if they are willing to share.

Again as a class, brainstorm what cyber bullying is, exploring the 7 different forms of cyber bullying: by text message, email, instant messenger (IM), websites, phone call, picture/video message, chat rooms.

Activity 2: Differences and similarities 15 mins

In small groups, ask pupils to use **Resource 11 – Differences and Similarities worksheet** to record how bullying and cyber bullying is the same, and how it differs. You may need to prompt pupils to consider:

- The feelings of the people involved (not just the victim, but also the bully and bystanders)
- The way in which the bullying is done / type of bullying
- Where it takes place
- How and where they would seek help

Ask pupils to feedback answers to the class as a whole and compare.

Activity 3: Cyber Bullying Film 20 mins

Show the cyber bullying film entitled 'Let's Fight it Together' which can be downloaded from www.digizen.org/cyberbullying/film The film is 6 minutes long. Staff are encouraged to view the film first before showing pupils to ensure it is suitable for their pupils. CAB recommend that the film be showed to upper KS2 only, but encourage you to make your own judgements, depending on the maturity of your pupils and the prevalence of cyber bullying in your class. The film follows a main character who is experiencing cyber bullying from classmates via threatening messages on his mobile phone and whilst chatting online, and eventually there is police involvement. Some pupils may find this distressing.

After watching the film, discuss with pupils what they would do if they were in Joe's position. Discuss who they can talk to or tell, and practical steps they could take – e.g. saving texts and messages, reporting cyber bullying to the police or internet / phone providers, etc. Discuss the role of bystanders in continuing cyber bullying or stopping it (e.g. telling someone, not passing messages on, not laughing along with others, etc).

Inform pupils that your school has an Anti Bullying Policy, providing a copy if possible. Discuss what the rules and punishments for being involved in bullying are in your school, ensuring children are aware that cyber bullying will also be punished.

Conclusion 5 mins

Recap on the main points discussed – cyber bullying IS bullying, but may take different forms. Cyber bullying can be a criminal offence and is very serious. We all have a role to play in combating cyber bullying and there are many different ways to seek help and report it.

Opportunity for assessment: Most pupils should be able to:

- Understand the definition of bullying and cyber bullying, exploring the differences and similarities.
- Identify the 7 types of cyber bullying and know what to do if it were happening to them or someone they know.
- Understand the bystanders role in contributing to, or preventing, cyber bullying.
- Understand the schools' sanctions and rules about bullying, including cyber bullying (anti bullying policy).
- Contribute to class and group discussions, verbalising thoughts and feelings.

Teacher Notes:

Key Stage 1 Questionnaire

Age:……

Boy ◯

Girl ◯

1) Do you have a **computer**?

Yes ◯ No ◯

2) Do you use the **internet**?

Yes ◯ No ◯

3) Do you **talk** to friends on the internet?

Yes ◯ No ◯

4) Do you play **games** on the internet?

Yes ◯ No ◯

5.) Do you use **email**?

Yes ◯ No ◯

6.) Do you have a **mobile phone**?

Yes ◯ No ◯

PTO

This questionnaire has been adapted from the Think u Know questionnaire which can be found on www.thinkuknow.com

Key Stage 2 Questionnaire

Please read first
Think u Know would like to know more about how you use the internet. You can help us learn more by filling out this questionnaire. We do not ask for your name, so your answers will remain anonymous; we do not share your answers with anyone else so they remain confidential - If you have any questions please ask your presenter. Thank you!!!

Age:…… **Boy** ◯
Girl ◯

1.) How often do you use the internet**?**

Every day ◯ More than once a week ◯ Once a week ◯ Once a month ◯ Less than once a month ◯

2.) If you use it every day how many hours do you use it for?

Less than 1 hour a day ◯ 1 – 2 hours ◯ 2 – 3 hours ◯ 3 – 4 hours ◯ More than 4 hours a day ◯

3.) What do you like doing the **most** online**? Choose one.**

Chat Rooms ◯ Blogs ◯ Music (e.g. iTunes) ◯ News ◯

Instant Messenger (MSN, Yahoo) ◯ Gaming ◯ File sharing (e.g. Limewire) ◯ Internet TV ◯

Social Networking (Bebo, Myspace) ◯ Web Browsing ◯ Shopping ◯ Other (Please specify) ……

4.) Do you play **games** on the internet?

Yes ◯ No ◯

PTO

5.) What websites do you play **games** on the most? **Choose one**.

BBC Games ◯ Miniclip ◯ Runescape ◯ XBOX Live ◯

World of Warcraft ◯ Nintendo Wii ◯ Neopets ◯ Playstation Online ◯

Club Penguin ◯ Other (Please specify)

.....

6.) Do you use **social networking** sites like Bebo and Myspace?

Yes ◯ No ◯

7.) What **social networking** site do you use the most? **Choose one**.

Bebo ◯ Myspace ◯ Facebook ◯ Faceparty ◯

Friendster ◯ Piczo ◯ Profile Heaven ◯ Other (Please specify)

.....

8.) Do you use **social networking** sites on your **mobile phone**?

Yes ◯ No ◯

9.) Do you use **Instant Messenger** (MSN, Yahoo) on your **mobile phone**?

Yes ◯ No ◯

10.) Do you use websites like youtube and Wikipedia?

Yes ◯ No ◯

Resource 2: How We Communicate

Name: _____ Date: _____

Type of communication	When would we use it?	Who would use it?
Home phone		
Mobile Phone		
Email		
Letter		
Text Message		
Poster		
Leaflet		
Chat room		
Instant Messenger (e.g. MSN)		
Social Networking Site (e.g. Bebo)		

Resource 3 : Who Would You Tell?

Name: _____ Date: _____

Look at the following pieces of information that someone might ask you for. Cut each one out, and decide who you would tell each piece of information to, matching up the information with the person on page 2. You might give some information to more than one person, or even lots of people.

First Name

Last name

School

Address

Phone number

Email address

Favourite colour

Your hobby

Favourite sports team

Date of Birth

City you live in

Star Sign

Age

Your friends names

Your password for your email and MySpace accounts

Now, cut out these descriptions of different types of people and decide what information you would tell them, placing the information labels next to each person. Some information might be given to more than one person.

Your Teacher	Your friend's mum
Chat room friend	A lady on the bus
Your best friend in school	A shop assistant
The bus driver	Your cousin
The doctor	An old man and woman waiting in a queue
A man in the street	
A policeman	
Competition on a website	

Resource 4: Personal!

Cut out the following 'Personal!' cards to be used in lesson 3, activity 1. One card is needed per pair or group of three.

Personal!

Personal!

Resource 5: SMART Thinking

S	Safe	Keep safe by being careful not to give out personal information (such as name, email address, phone number, home address or school name) to people who you don't trust online.
M	Meeting	Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission, and even then only when they then go with you.
A	Accepting	Accepting emails, IM messages or opening files, pictures or texts from people you don't know or trust can lead to problems. They may contain viruses or nasty messages.
R	Reliable	Someone online may be lying about who they are, and information you find on the internet may not be reliable.
T	Tell	Tell you parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. They can help you to report at www.thinkuknow.co.uk, and talk to someone who can help.

STOP and THINK

Resource 6: Statements & Scenarios

You know who you're talking to because you can see them

You can talk to someone can talk to someone in another country

You don't know who you're talking to because you can't see them

You can pretend to be someone you're not

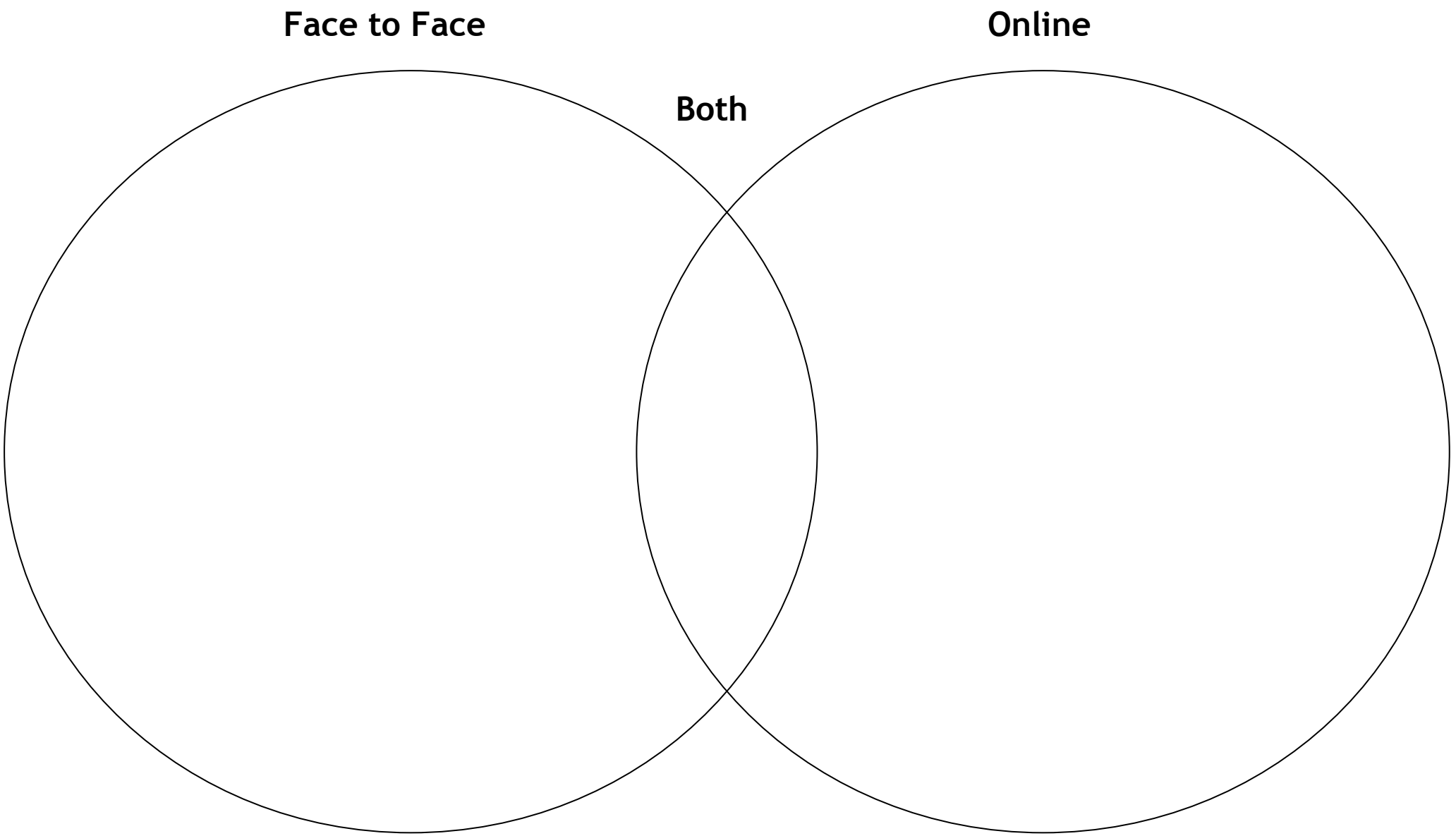
You can tell what sort of age the person is

You can't always tell if they are joking or serious

It's easy to tell what people mean because you can hear the tone of their voice

You must think carefully about giving them personal information, such as where you live

Resource 6: Statements & Scenarios



Resource 7: Trusting Content Quiz

Children will need access to the internet, either individually or in small groups to complete this exercise.

Pupils will need to use a search engine to find the answers to these questions. You may wish to ask different groups to use different search engines, to see if this has an effect on the answers.

Ask pupils to record their group's answers on the accompanying worksheet, 'Resource 8: Quiz Answers' noting their answer, where they found the information (web address) and which search engine they used to find the information.

Question 1

How many miles away from the Sun is Earth?

Answer: 93 million miles

Question 2

In what year was Christmas banned in Britain?

Answer: 1647 AD

Question 3

Who was the second person to walk on the moon?

Answer: Edwin Eugene (Buzz) Aldrin, Jr

Question 4

What was the best selling single of 2007?

Answer: Leona Lewis – 'Bleeding Love'

Question 5

What is the name of Jacqueline Wilson's latest novel?

Answer: Cookie (October 2008)

Question 6

What was the lowest temperature ever recorded in the world? Extra point for saying where it was recorded!

Answer: -89.2 C (-128.6 F) on the 21st July, 1983 recorded at Vostock, Antarctica

Question 7

What is the most amount of money paid for a work of art?

Answer: This question doesn't have a clear answer. It would appear to be Jackson Pollock's 'No. 5, 1948' which sold for $140m (£73.35m) in November 2006; followed closely by $135m paid for a portrait by Klimt. However, the question doesn't state whether it's a work of art by a living or deceased artist – (living artist: Lucian Freud, $33.6 million)

Question 8

Who is the highest paid actor?

Answer: The answer appears to be Will Smith who earned 80 million dollars in 2008. However, this information often changes. The highest paid actress appears to be Reese Witherspoon, earning $15-$20m per movie.

Question 9

What is the most spoken language in the world?

Answer: Different answers are provided on different websites, so it is difficult to find an accurate answer online. Most sites suggest the answer is Mandarin with 1 billion + speakers worldwide, followed by English with 510 million speakers worldwide.

Question 10

How many children get bullied in the UK each year?

Answer: There is no answer to this! There are a number of different figures, depending on if children report they are being bullied to someone, which many don't. Some surveys suggest that as many as 9 out of 10 children are bullied at some point in their lives*, other say as few as 4 in 10.*

Resource 7: Trusting Content Quiz

Names of people in this group: _____ Date: _____

Write your answer in the box below, with the website address of where you found the information and which search engine you used.

Q	Answer	Web address	Search Engine Used
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Resource 8: Comparing Websites

Website Address	Description of website (is it providing information, news, is it educational, for fun, games, selling something?)	Who is it aimed at? (What age of person is it aimed at? What type of person would use this site?)	Is it attractive and user-friendly? Why? (Think about colours, layout, how easy it is to use and find what you need)	Would you use this site? Why?	Does this site contain anything that you don't trust or you're unsure of?

Resource 9: Case Study

Read the following case study about Abby and use the worksheet (Resource 10) to answer the questions.

Abby is 10 years old and is in class 6 at Hillrise Primary School. She really likes spending time with her friends, in school and outside of school in the evenings and weekends. Abby recently was given a new laptop by her mum and dad. She has started using the new laptop a lot in the evenings to surf the internet. Abby has joined a few different chat rooms to speak to people who are interested in the same things as her.

Abby has been chatting to a few different people in a music chat room. She has been talking to someone called Si_693 who has told Abby that his name is Simon and he's 12 years old. Simon asked Abby what sort of music she was into and they seem to have a lot in common. Simon and Abby were talking about a particular pop group who were having a U.K. tour.

Si_693

Hey Abby! Have you heard?! Scuzz Buddies are touring!

Abigail_Potter2

Hey! ☺ Yeah I heard! Is that cool or what! I can't wait to see them live.

Si_693

Are you going to get tickets? Which show are you going to?

Abigail_Potter2

The one in Bristol. I asked my dad to get them for me for my birthday.

Si_693

No way! Me too! We should go together! When's ur birthday? Dyou live in Bristol then?

Abigail_Potter2

Yeah. It's my birthday on Friday.

Si_693

Cool me too! Which school dyou go 2 then?

Abigail_Potter2

Hillrise Primary….I think I g2g my mum's calling me

Si_693

Don't go yet, we got2 talk bout the tour

Abigail_Potter2

Ok, just quickly then

Si_693

We should book our tickets at the same time so we can sit together – hey I tell U what, let's meet up nxt wk and talk bout it.

Si_693

Where'd u live?

Abigail_Potter2

I can't tell you

Si_693

Why not! We r friends aren't we?

Abigail_Potter2

Yeah…

Si_693

So tell me! Well meet me in the park then….Do you live near Meadowlane Park?

Abigail_Potter2

Yeah…

Si_693

Ok well I'll meet you in there then - after school on Friday?

Abigail_Potter2

Ok. C U then.

Abigail_Potter2 has left the chatroom

Resource 10: Case Study Worksheet

Using the Case Study about Abby and Simon, answer the following questions.

1. ***What personal information did Abby give to Simon?***

2. ***What personal information did Simon give to Abby?***

3. ***Why do you think Abby gave that information?***

4. ***Why is it not a good idea to give out personal information in chat rooms?***

5. ***What could Abby have done instead?***

6. ***What could Abby do now if she was worried?***

7. ***Who can Abby tell if she is worried or upset?***

8. ***Was Abby's chatroom name an example of a safe name to use whilst chatting?***

Resource 11: Bullying & Cyber Bullying

Work with a partner or in a small group to think about ways in which bullying and cyber bullying are **similar** and **different**, recording your answers below.

	Bullying	**Cyber Bullying**
Describe what it is		
Who might be affected?		
Where is it most likely to take place?		
How would a person feel if someone were doing this to them?		
Who could they tell?		
What would they do about it?		

Bibliography

Websites:

www.cardiffagainstbullying.co.uk

www.thinkuknow.co.uk

www.cybersmart.org

www.digizen.org

www.bbc.co.uk/webwise

www.stopcyberbullying.org

www.direct.gov.uk/cyberbullying

www.anti-bullyingalliance.org.uk

www.netsmartz.org

www.childnet-int.org/kia

www.kidsmart.org.uk

www.becta.org.uk

www.wisekids.org.uk

www.cybermentors.org.uk

www.wales.gov.uk

www.ceop.gov.uk

Books:

Cyber-Safe Kids, Cyber-Savvy Teens: Helping young people learn to use the internet safely and responsibly
Nancy E. Willard

(2007) Jossey-Bass Publishing ISBN: 978-0-7879-9417-4

Guidance:

Cyberbullying - Safe to learn: Embedding anti-bullying work in schools
Department for Children, Schools & Families

This resource can be downloaded at
www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Signposts to Safety: Teaching e-safety at KS 1/2 & 3/4
Becta

This resource and others can be downloaded at:
http://schools.becta.org.uk/index.php?section=is

Cardiff Against Bullying (CAB)
Bryn Y Deryn , The Mynachdy Centre,
Cefn Road, Cardiff CF14 3HS

(029) 2061 7632 CAB@cardiff.gov.uk

This document has been produced by Cardiff Against Bullying (CAB) and the Cardiff I.T. Advisory Services on behalf of Cardiff Council.

April 2010