HEATHER RIDGE
INFANT SCHOOL

E-SAFETY POLICY

Governor Committee Responsible	**N/A**
Review period	**ANNUAL**
Policy approved by Governors/Head Teacher	**HEAD TEACHER**
Meeting minute reference	
Status	**STATUTORY**
Next review	**Autumn 2019**
Document version number	**V1.3**
Author	**Sarah Elliott**
Contributors	**SURREY COUNTY COUNCIL**
To be read in conjunction with the following policies	**Computing Policy** **Anti-bullying Policy (Cyper)**

Document History	
V1.0	
V1.1	Oct 14
V1.2	Nov 17
V1.3	Nov 18

Introduction

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

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

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At ***Heather Ridge Infant School,*** we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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

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

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

School Aims

The e-safety Policy is part of the School Development Plan and relates to other policies including those for IT, anti-bullying and for child protection.

- The school will appoint an e-safety coordinator. In some cases this will be the Child Protection Liaison Officer as the roles overlap. In our school the e-safety coordinators are Sarah Elliott and Jo Ford.
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school internet access is provided by Surrey County Council through a regional broadband contract, which includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate internet content

- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content.
- For children with social, familial or psychological vulnerabilities, further consideration will be taken to reduce potential harm.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Managing internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Pupils are not provided with school email addresses in our school.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication is not allowed; emails to parents via school email accounts is permitted.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Publishing pupils' images and work
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking

- The school do NOT permit the usage of social networking sites in school
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location when using networking sites out of school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites outside of school.

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents may be useful to identify patterns and behaviours of the pupils.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras are not permitted by pupils in school.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. These are not permitted in school.
- Staff will use a school phone where contact with pupil parents is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GPDR.

Authorising internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Community use of the internet

All use of the school internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications

Introducing the e-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as students become more mature and the nature of newer risks can be identified.

Staff and the e-safety policy

- All staff will be given the School e-safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents' support

- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents should be given e-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

Appendix 1

Heather Ridge Infant School Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school's email / Internet / Website and any related technologies for professional purposes or for uses deemed "reasonable" by the Head or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without seeking permission from the headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ………………………………………………………… Date …………………………………………

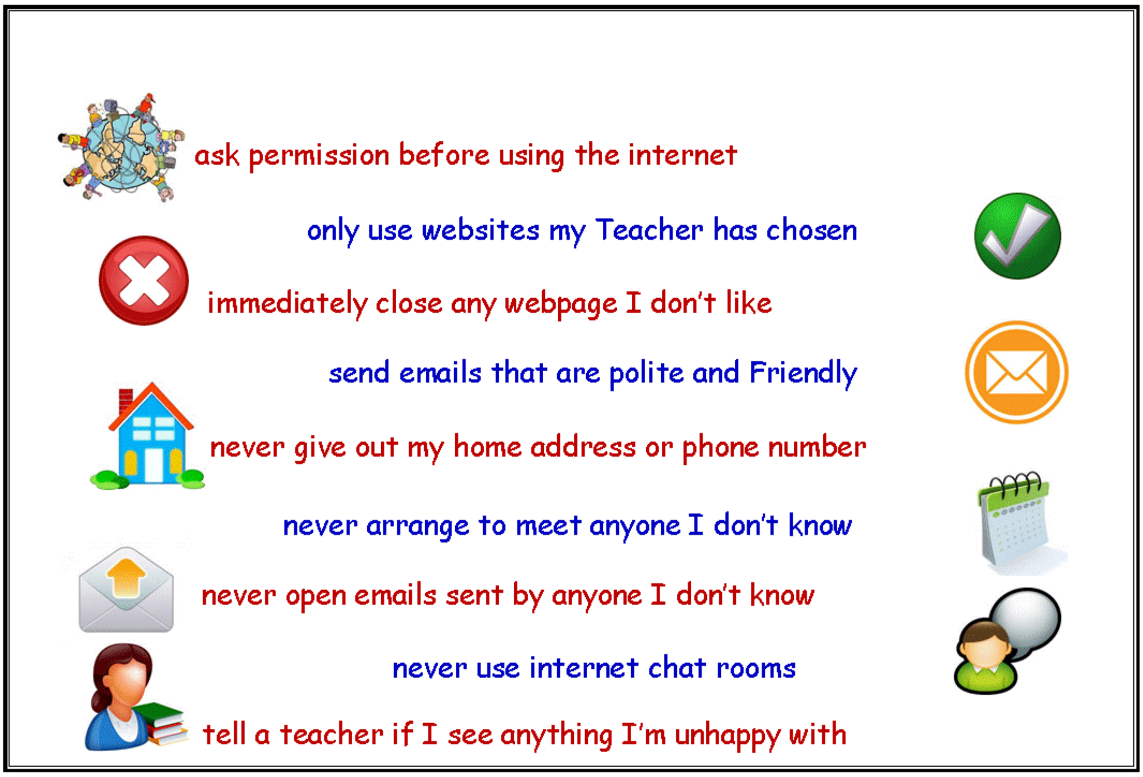
Full Name ……………………………………………………… (printed) Job title …………………………………………

Appendix 2

Heather Ridge Infant School

PUPIL E-SAFETY AGREEMENT

As a pupil at Heather Ridge Infant School I agree to:



ask permission before using the internet

only use websites my Teacher has chosen

immediately close any webpage I don't like

send emails that are polite and Friendly

never give out my home address or phone number

never arrange to meet anyone I don't know

never open emails sent by anyone I don't know

never use internet chat rooms

tell a teacher if I see anything I'm unhappy with

Appendix 3

Heather Ridge Infant School
Parent/Carer consent form and e-safety Rules
All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the e-safety Rules have been understood and agreed.
Parent / Carer name: ……………………………………………………………
Pupil name: ………………………………………………………………………….
As the parent or legal guardian of the above pupil, I have read and understood the attached school e-safety rules and grant permission for my daughter or son to have access to use the internet and other IT facilities at school.

I know that my daughter or son has read/or I have read a copy of the school e-safety rules. We have discussed this document and my daughter or son agrees to follow the e-safety rules and to support the safe and responsible use of IT at Heather Ridge Infant School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their e-safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent/Guardian signature: ………………………………………………………….Date…………………………………………….
Please complete, sign and return to the school office

Appendix 4

E-safety rules & sanctions

E-safety rules and sanctions

It is appropriate for people to be allowed a great deal of freedom in using IT for study, work and leisure. With freedom comes responsibility. **Heather Ridge Infant School** cannot control what people, all over the world, make available on the internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect all IT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of IT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's internet filtering
- Not to download or even try to download any software without the explicit permission of a member of the IT systems support department
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the IT Facilities
- To report any breach (deliberate or accidental) of this policy to the class teacher immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Heather Ridge Infant School reserves the right to access all material stored on its IT system, including that held in personal areas of staff and pupil accounts for purposes of ensuring DfE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the IT facilities. Heather Ridge Infant School will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the IT facilities – on a permanent basis.

Sanctions for the misuse of Heather Ridge School IT facilities

First Offence

- With an adult, the pupil will need to read the IT AUP to ensure they are clear about the regulations by the completion of an educational worksheet.
- The e-safety Co-ordinator will write a letter to parents (or phone if preferred) to inform them of the breaking of the IT AUP.
- The relevant Year Leader and an appropriate senior member of staff will be informed.
- The incident and response will be logged.

Second Offence

- The e-safety co-ordinator will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the second time. The letter may include specific information about the offence.
- The pupil will have restrictions placed on their use of the IT facilities by the removal of internet access for one week.
- The pupil may receive a further sanction depending on the nature of the offence.
- The relevant year leader and appropriate senior member of staff will be informed.
- The incident and response will be logged.

Third Offence

- The pupil will have their internet access removed immediately by the e-safety Co-ordinator for a minimum of 4 weeks.
- The e-safety Co-ordinator will write a letter to parents and phone them to inform them of the breaking of the IT AUP for the third time. The letter will ask parents to come into school to discuss the breaking of the IT AUP with the e-safety Co-ordinator.
- The pupil will have a meeting with the e-safety Co-ordinator and the Deputy Head teacher to discuss the breaking of the IT AUP and the subsequent sanction.
- The relevant year group leader and senior member of staff will be informed.
- The incident and response will be logged.

Appendix 5

Use of digital images

To comply with the Data Protection Act 1998, we need parental permission to use photographs or recordings of any child.

When posting images for external use, we will avoid using surnames.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress will be used.

Staffs are not allowed to take photographs or videos on their personal equipment.

There are many opportunities for digital imagery to be used, for example, during a learning activity to demonstrate or evaluate work, to present work to others, to share good practise with the wider community, to celebrate achievements and many more.

These may be displayed on our website, which is public facing and could potentially viewed by anyone on the internet, or they may be displayed on our virtual learning environment, which is private to the school community and can only be viewed by those with a username and password.

We would like to ask your permission for

Use of digital images - photography and video:

I agree to the school using photographs or videos of my child
____ (name)

On the public facing website: yes / no (please circle)

On the privately accessed VLE: yes / no (please circle)

I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: ___________________________ Date: ___/___/___

Appendix 6

Responding to an e-safety incident

This guidance is for senior management within schools on how to respond to an e-safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.

The first section outlines key e-safety risk behaviours. The flowchart on page 4 illustrates the approach to investigating an incident of concern. This diagram should be used with the screening tool and the Surrey Child Protection Procedures which include what to do if you are concerned about a child, or about an adult working with children. Schools' CPLOs will be conversant with these and the processes for referral.

What are the e-safety risks?

The explosion in technology over the last 10 years, in particular the internet, has provided endless opportunities for children, young people and adults to gain access to information and to communicate with each other. The internet is an unmanaged, open communications channel, via which anyone can send messages discuss ideas and publish material – and it's these very features which make it an invaluable resource used by millions of children every day. But it is these same features which present a number of risks to children. The vast majority of children's experiences will be positive - but we must be aware that this new technology can be used to bully others, and be manipulated by people who wish to do harm to children.

What does electronic communication include?

- internet collaboration tools (e.g. social networking sites, blogs)
- internet Research (e.g. web sites, search engines and Web browsers)
- Mobile Phones and personal digital assistants
- internet communications (e.g. E-mail and Instant Messaging)
- Webcams and videoconferencing

Risk Behaviours:

Online grooming and child abuse

There are a number of illegal actions that adults can engage in online that put children at risk: 50

- Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught
- Swapping personal information of children that they have collected with other abusers
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex

Cyberbullying

In addition to face-to-face bullying, bullying via technology is becoming increasingly prevalent. A Beatbullying survey in 2017 found that:

- 39% had a nasty comment posted on their profile
- 34% had a nasty comment posted on their photo
- 68% had been sent a nasty private message
- 18% had their profile wrongfully reported
- 23% had been bullied in an online game
- 24% had their private information shared
- 18% had somebody impersonate them online
- 41% had rumours about them posted online
- 27% had photos/videos of them that they didn't like

"Cyberbullying" is the use of Information and Communications Technology, ICT, particularly mobile phones and the internet, deliberately to upset someone else. "Cyberbullying" is when a child or young person is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or young person (or group) using the internet, interactive and digital technologies or mobile phones.

It can be an extension of face to face bullying, with technology providing the bully with another route to harass their target. It differs in several ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity. The 'usual' boundaries of face-to-face bullying are not observed – the bully is not restricted by the size, age or location of their victim.

Inappropriate or illegal content

Because it's so easy to upload information onto the internet, much online content is now inaccurate or extreme – yet is often presented as fact. A great deal of the material on the internet is published for an adult audience, and some is unsuitable for children. For example, there is information on weapons, crime and racism, access to which would be much more restricted elsewhere.

Disclosing personal information and identity theft

Publishing personal information about themselves online could compromise children's security, and that of those around them. Furthermore, as soon as a message is sent or an image is posted, it can be shared, copied and changed by anyone. Children need to think carefully about their online 'etiquette'.