Safety in a Digital World:
Guidance and Acceptable Use Policies Template

An E-safety Toolkit
Contents

1.0 Introduction

1.1 An E-safety Strategy for Hull
1.2 National Context
1.3 What do we mean by E-safeguarding?
1.4 The place of Acceptable Use Policies
1.5 The Hull E-safety Toolkit

2.0 Guidance and Policy Template

2.1 Empowering Children and Young People in the Digital World

2.1.1 Why is Internet use important?
2.1.2 How does Internet use benefit children and young people?
2.1.3 How can we ensure Internet use enhances learning and life experience?
2.1.4 How will children and young people learn how to evaluate content?

2.2 Managing Information Services

2.2.1 How will information systems security be maintained?
2.2.2 How will filtering be managed?
2.2.3 How will videoconferencing be managed?
2.2.4 How can 'emerging technologies' be managed?

2.3 Privacy and Protection

2.3.1 How should personal data be protected?
2.3.2 Password security
2.3.3 How will email be managed?
2.3.4 How will published content be managed?
2.3.5 Can pupil images and work be published?
2.3.6 How will social networking and personal publishing be managed?

2.4 Risks and Responses

2.4.1 How will Internet access be authorised?
2.4.2 How will risks be assessed?
2.4.3 How will complaints be handled?
2.4.4 How should the Internet be used across the community?
2.4.5 How will Cyberbullying be managed?
2.4.6 How will Learning Platforms and VLEs be managed?
2.4.7 Response to an Incident of Concern
2.4.8 Incident Log sheet
2.4.9 Response to risk Flowchart

2.5 Communications
2.5.1 What should the communications plan contain?
2.5.2 How will the policy be introduced to children and young people?
2.5.3 How will the policy be discussed with staff?
2.5.4 How will parents’ support be enlisted?

3.0 Implementing Acceptable Use Policies
3.1 Development Planning
3.2 Organisational Roles
3.2.1 Who will write and review the policies?
3.2.2 How are the policies reviewed in Hull?
3.3 Education and Training
3.4 E–Safety Audit

4.0 Appendices
4.1 Example AUPs
4.1.1 Safety in a Digital World: Guide for Professionals
4.1.2 Safety in a Digital World: Guide for Parents/Carers
4.1.3 Safety in a Digital World: Guide for Children and Young People
4.2 Legal Framework
4.3 Useful Links and Contacts
4.4 Glossary
4.5 Publicity material and other resources

5.0 Acknowledgments
“Children and young people need to be empowered to keep themselves safe - this isn’t just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim”

(Byron Review: 2008). ¹

www.dcsf.gov.uk/byronreview/actionplan
An E-safety Strategy for Hull.

New technologies are creating fantastic, exciting opportunities in communication, in learning and in many aspects of daily life. For young people they are a regular and familiar part of everyday life that is being enthusiastically embraced. For many adults these developments seem quite different from what we have seen before. This makes us naturally cautious about them. This gives those of us whose role it is to safeguard our children and young people new considerations, challenges and responsibilities.

We are clear about this responsibility in Hull. Under the guidance of the Hull Safeguarding Children Board E-safety work-stream we have developed the E-safety Strategy to give coherence and focus to our work, providing a safe, city-wide framework. The E-safety Strategy recognises the role developments in digital technology play in shaping the way young people access ICT, highlighting the importance of helping young people understand what constitutes acceptable use. Crucially, it focuses on building the resilience of young people in using digital technology, so they are equipped to enjoy the benefits whilst avoiding the pitfalls and dangers.

We must personalise the support we provide to ensure each child or young person has the skills and understanding to use digital technology safely. We must seek the participation of children, young people and families so we can appreciate the changing nature of their usage and respond accordingly. We must work in partnership to deliver a coherent approach with a particular focus on bringing everyone together around this common agenda. Finally, we must come back to our responsibility – prevention - helping young people to ensure that they are able to identify, avoid and report dangers before they escalate.

We all have a duty to safeguard and promote the well being of all children. This duty of care cannot be confined to a single environment. E-safeguarding must extend to all environments in which children and young people actively engage with the digital world, in school, at home or through personal use within the community. This requires an integrated approach.

Our strategy is to develop safety and responsibility in the digital world and to educate and empower children and young people to identify and mitigate risk. The strategy requires all professional organisations, parents/carers, pupils and others to sign-up to the principles contained within this document, the policies underpinning it and to safeguarding children in the digital world.

Independent Chair, Hull Safeguarding Children Board
The Hull E-safety Toolkit:

There are many aspects to keeping safe online. All agencies and organisations working with children and young people will be dealing with the policies, infrastructure and education they need to put in place to ensure e-safety at a personal, network, data security and organisational level. Parents/carers will need to understand the risks their children may be exposed to, and how they can supervise and support their children effectively. Young people themselves will need to develop the skills to evaluate the way they use technology at home and at school, identify those risks and develop ways to balance the risks with the benefits. In responding to the challenges above, the Hull E-safety Toolkit has been produced, including Guidance and Policy Documentation, exemplar Acceptable Use Policies (AUPs), and assistance in raising public awareness.

What do we mean by e-safeguarding?

E-safeguarding procedures address all safeguarding issues which relate to the use of digital technology. There are two main elements to these issues:

1. **E-safety**
   E-safety means ‘electronic safety’, it is not just about keeping safe on the internet but also keeping safe on all electronic devices such as mobile phones, television, games consoles, tablets and PCs and laptops. All organisations require procedures to understand rights and responsibilities in using digital technology safely. These procedures should be expressed in the organisation’s Acceptable Use Policy (AUP).

2. **E-security**
   E-security refers to the protection of data against the deliberate or accidental access by unauthorized persons, and also includes protection against accidental damage or loss. All organisations require procedures to protect the physical network infrastructure to ensure all information and electronic data is securely maintained and is categorised as Public, Restricted or Protected.

![Diagram of Hull Safeguarding Children Board Guidance](image-url)
Guidance and Policy Template:

National Context:

The Byron Review Safer Children in a Digital World: The Report of the Byron Review 2008, investigated the issues and opportunities for keeping children and young people safe in their use of digital technologies. The report highlighted the benefits the digital world provides but also the risks surrounding potentially inappropriate material. Such online risks can be classified in terms of **content**, **contact** with others and **conduct** of children in the digital world, illustrating that e-safety risks are posed more by behaviours and values online than the technology itself. As such, a child may be a recipient, participant or actor in online activities posing risk, as evident in Figure 1 below.

![Figure 1 - developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review.](image)

The Byron report concluded that our approach to children and young people’s use of technology must shift: rather than restricting access to technology, we need to not only ‘reduce the availability of potentially harmful material’ but also, ‘restrict access to it by children’ and ‘increase children’s resilience’ and in doing so empower children to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online.

Professor Byron began her progress review in January 2010 and on 29 March 2010 published “Do we have safer children in a digital world? A review of progress since the 2008 Byron Review”.

Key recommendations from the progress review include:-

- Raise public awareness;
- Improve e-safety education.
The Template:

This section of the Hull E-safety Toolkit provides a template that contains guidance and suggested statements for those providing services to children and young people including educational establishments within Hull to use in the formulation of a working Acceptable Use Policy.

E-safeguarding requirements are expressed in two ways:

1. **Mandatory elements:** All statements with the word ‘shall’ are mandatory and are printed in **bold italics**.

2. **Recommended elements:** All statements with the word ‘should’ are recommended as good practice.

Both mandatory and recommended elements form the policy statements for educational establishments and those providing services to children and young people within Hull.

In responding to this template, organisations are invited to establish HOW they will implement the mandatory and recommended elements. The outcome of this response will be the creation of working procedures, understood and adopted by all – through Acceptable Use Policies (AUPs).

It is anticipated that educational establishments and those providing services to children and young people within Hull will take this template and produce their own guidance and policy documents. These will be used as reference alongside working and understandable Acceptable Use Policies.

The guidance inserts *(name of organisation)* where organisations within Hull will wish to insert their own title.

Some sections are more appropriate to educational establishments, some to other services. It is important that individual institutions customise the template to provide clear guidance, directed at their specific requirements.

It is important to include a statement regarding who has been involved in the writing of your E-safety Guidance and the Acceptable Use Policies and the guidance you have used to assist in its development. The statement below can be adopted for this purpose:

Our E-safety Guidance and Acceptable Use Policies have been written by *(name of organisation)*. They build upon the Hull City Council’s (HCC) E-safety Policy and government guidance and are in accordance with Hull Safeguarding Children Board’s Guidelines and Procedures which can be accessed via [http://www.proceduresonline.com/hull/scb/](http://www.proceduresonline.com/hull/scb/) It has been agreed by *[who has agreed this within your organisation, e.g. Manager, Head of Service, Headteacher]* and approved by *[who has approved this within your organisation e.g. Governing Body, Head of Service, City Council]*.
Risks and Responses:

How will risks be assessed?
E-safety is based upon the assessment of risk and the implementation of controls to manage these risks. The organisation will need to address the issue that it is not possible to completely remove the risk that children and young people might access unsuitable materials via the internet. Information security is critical, in both protecting the information held concerning staff/volunteers, children and young people, and in ensuring the reliability of ICT systems to support teaching, learning and internet access.

As a minimum, the risk assessment shall be updated and reviewed annually by the Senior Leadership Team/Senior Manager of the organisation and reported to the Governing Body/Trustee. It is recommended that a review should be conducted each term. It is wise to include a disclaimer, an example of which is given below.

Policy statements:

- **(Name of organisation)** will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither **(name of organisation)** nor HCC can accept liability for the material accessed, stored or distributed or any consequences resulting from Internet use.
- **(Name of organisation)** should audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will Internet access be authorised?

The organisation should allocate Internet access for staff members/volunteers, children and young people on the basis of educational need. It should be made clear to staff who has Internet access and who has not. It should also be made clear to users when they have Internet access and when they have not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage should be fully supervised, all children and young people in a class could be authorised as a group. Normally most children and young people will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission shall be required for Internet access in all cases — a task that may be best organised annually when children and young people’s home details are checked and as new children and young people join.

Possible statements:

- The organisation will maintain a current record of all staff/volunteers, children and young people who are granted access to the organisation’s electronic communications systems.
- All staff/volunteers must read and sign the organisation’s policies regarding information security and the use of information technology before using the organisation’s ICT resource.
• For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
• Young people must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy.
• Parents/carers will be asked to sign and return a consent form for children and young people’s access.
• Parents/carers will be informed that children and young people will be provided with supervised and unsupervised Internet access, but must comply with the AUP at all times.

**How will social networking and personal publishing be managed?**

Social networking sites connect people and provide an online community to which a young person may wish to belong, or a ‘place’ they may wish to visit, this may involve them being exposed to risk. Social networking sites provide easy to use, free facilities; users can publish unmediated content and are invited to view personal ‘profiles’, communicate and leave comments, over which there may be limited control.

Children and young people should be encouraged to think about the appropriateness of uploading personal information and the associated dangers, including the difficulty of removing an inappropriate image, video or information once uploaded and published.

All adults should be made aware of the potential risks of using social networking sites or personal publishing in a professional capacity both with children and young people or personally. This should include the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social networking include: blogs, wikis, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger, Facebook, Twitter, Club Penguin, Moshi Monsters and Habbo Hotel (it is impossible to provide a comprehensive list as the digital landscape develops quickly).

**Possible statements:**

• *(Name of organisation)* will control access to social media and social networking sites.
• Children and young people will be advised never to give out personal details of any kind which may identify them and/or their location to persons unknown or through unsecured sites. Examples would include their real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
• Children and young people should be advised not to place personal photos or videos on any unsecured social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail (such as a school crest) in a photograph or video which could identify the child or young person or his/her location.
• Organisational blogs or social media sites should be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager. Employees/volunteers should be advised not to run social network spaces for children and young people’s use on a personal basis.
• If personal publishing is to be used with children and young people then it must use age appropriate sites suitable for educational purposes and the site should be moderated by organisational staff.

• Children and young people should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children and young people should be encouraged to invite known friends only and deny access to others by making profiles private.

• Children and young people are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will issues be managed?

How will child sexual exploitation and ‘grooming’ be managed?
Child sexual exploitation is when someone grooms and controls a child for a sexual purpose. The terms 'child sexual exploitation' or the 'commercial sexual exploitation of children' are used to refer to a range of illegal and abusive activities. These activities can be broadly separated into two areas:

• sexual exploitation through street grooming;

• online sexual exploitation.

Online sexual exploitation can include:

• grooming children online for the purpose of sexually abusing them. This might involve an adult pretending to be a child, befriending the child through online chat rooms, social networking websites, email, mobile telephone messaging, gaining their trust, stalking their online activities;

• asking children to participate in non-contact sexual activities such as engaging in sexual conversations online, via mobile telephone and/or via webcam;

• asking children to take and share indecent images of themselves online or through a mobile telephone;

• asking children to display sexualised behaviours or perform sexual acts that are recorded or shared live via webcam;

• the creation, storage and distribution of child abuse images (historically referred to as child pornography but more accurately as indecent images or images of child sexual abuse);

• arranging to meet a child in person for the purpose of sexually abusing them.

When responding to online grooming it is important to follow the HSCB ‘Incident Log’ detailed below. The definition of ‘Significant Harm’ must be adhered to in assessing and addressing the risk posed to children using online communications. The guidance in relation to social networking/media is particularly relevant in promoting safer practices online for children, parents/carers and staff.

Possible statements:
• *(Name of organisation)* will be vigilant in relation to child sexual exploitation and online grooming.

• Staff/Volunteers will be made aware of the organisation’s protocols and responsibilities in relation to online grooming including how and to whom to share information and concerns.

• *(Name of organisation)* will follow HSCB ‘Incident Log’ to record any issues.

• *(Name of organisation)* will report any concerns about a child’s safety to Children’s Social Care.

• *(Name of organisation)* will develop approaches to educate children, young people and parents on the dangers of online grooming and sexting.

• Sex and Relationship Education and/or PHSE may be an opportunity to explore issues including consent, sexting, appropriate relationships, pornography use and protective steps children and young people can take online.

How will ‘sexting’ be managed?

‘Sexting’ is defined in the South West Grid for Learning resource “So You Got Naked Online” as a term that “describes the use of technology to share personal sexual content”. This content can be anything from text only messages and/or images and video, including full or partial nudity right up to still or moving images of sexual acts. Often this practice is between consenting partners, but can be broadcast to groups using a whole range of devices, technologies and online spaces. However, the most common ones are mobile phone MMS, Skype and social network sites where images can be posted and shared (Facebook, Twitter, Tumblr, Flickr, YouTube etc). There have been attempts recently to try and move the term away from ‘sexting’ to the more accurate and less sensational “self—generated indecent images”, for example in the recent Internet Watch Foundation research.

Much of the research evidences that ‘sexting’ is prevalent and many children and young people are involved in this type of online behaviours. Due to this it is important that organisations, agencies and the LSCB have an appropriate response to it. Children sharing, storing and distributing images with sexually explicit content may be committing offences under the Sexual Offences Act 2003 and it is important that children are given clear messages about their online conduct and potential consequences.

Possible statements:

• *(Name of organisation)* will make children aware of the risks associated with the creating, storing and sharing of images of a sexual nature;

• There will be clear procedures in place to support anyone affected by ‘sexting’; including appropriate referrals to Children’s Social Care and/or the Police and organisational responses including
involvement of Child Protection Co-ordinators, E-safety leads and/or designated Safeguarding leads/teams.

• Sanctions for those involved in ‘sexting’ may include:
  • The individual will be asked to remove any material deemed to be inappropriate or offensive.
  • A service provider may be contacted to remove content.
  • Internet access may be suspended for the user for a period of time.
  • Parents/carers may be informed.
  • The Police will be contacted if a criminal offence is suspected.

---

Child Exploitation and Online Protection (CEOP)

Children and young people need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in your organisation who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support. Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.
How will Cyber-bullying be managed?

Cyber-bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” (DCSF 2007).

When children are the target of bullying via mobile phones, games consoles or the internet, they can often feel very alone, particularly if the adults around them do not understand cyber-bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. Previously bullying was often confined to school hours, cyber-bullying can be a constant intrusion into children’s lives.

It is essential that children, young people, organisations, and parents/carers understand how cyber-bullying is different from other forms of bullying, how it can affect children and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: http://www.digizen.org/cyberbullying.

Possible statements:

- Cyber-bullying (along with all forms of bullying) will not be tolerated in (name of organisation). Full details are set out in (name of organisation) policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by cyber-bullying.
- All incidents of cyber-bullying reported to (name of organisation) will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyber-bullying:
  - Children and young people, staff/volunteers and parents/carers will be advised to keep a record of the bullying as evidence.
  - (Name of organisation) will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyber-bullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended for the user for a period of time.
  - Parents/carers may be informed.
  - The Police will be contacted if a criminal offence is suspected.
The place of Acceptable Use Policies.

Effective Acceptable Use Policies (AUPs) are an essential tool to promote safe and responsible behaviours online in organisational settings, the home and for those who provide services to children and young people. AUPs state the way in which new and emerging technologies may and may not be used and the sanctions for misuse. It is important that AUPs are developed within a framework of wider e-safety measures within their local context. These measures involve the combined approach of effective policies and practice, a robust and secure technology infrastructure, and education and training for both children and adults alike, all underpinned by standards and inspection. A diagram of how AUPs relate to wider policies and procedures, including this document, is included here.

Implementing Acceptable Use Policies:

The responsibility for compliance for adopting, implementing, communicating and reviewing acceptable use policies resides with the organisation, a possible process to follow is listed:

1) **Appoint** an **E–safety Co-ordinator** (or equivalent) within the organisation.
2) **Provide** safeguarding and e-safety training for the **E–safety Co-ordinator** and staff within the organisation.
3) **Perform** a self-audit regarding e-safety.
4) **Use** Section 2 of this document as a policy template if required, and edit/customise for the organisation.
5) **Publish** the example AUPs provided or edit/customise for the organisation.
6) **Review** the e–safety policy and its implementation annually and whenever an e-safety incident occurs. Ensure that planning for the review is part of the e-safety Guidance.
7) **Notify** the relevant agencies/professionals when an e-safety incident occurs.

Organisations can seek advice and support from the Hull Safeguarding Children Board regarding the reviewing and updating of their E-safety Policy. The following section contains example AUPs:

1. Safety in a Digital World: Guide for Professionals:

Technology is provided and maintained for the benefit of all staff within [name of organisation] to enhance skills and become more effective in the workplace. You are encouraged to use and enjoy these resources, using the following agreement as a guide.

There is a need to ensure that digital technologies are used appropriately and for you to have an understanding of your responsibilities in keeping yourself and young people safe. This guide aims to assist you, making sure that you have all necessary measures in place.

Internet and Email:
- I agree to only access suitable material;
  I am aware that accessing materials which are unlawful, obscene or abusive is not permitted.
- I agree to report unsuitable material;
  If I receive an email containing material of a violent, dangerous, racist, or inappropriate content, I will always report such messages to the E-safety Co-ordinator.
- I agree to the professional code of behaviour;
  I appreciate that other users might have different views from my own and acknowledge that the use of strong language or aggressive behaviour is not acceptable.
- I agree to keep within copyright laws;
  I will respect work and ownership rights of people, including abiding by copyright laws.
- I agree to the responsible use of social networks, both within and outside the workplace;
  The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.

Equipment:
- I agree to take care to protect hardware and software;
  This includes protecting the ICT equipment from spillages by eating or drinking well away from them. I will always get permission before installing, attempting to install or storing programs of any type on the ICT equipment. I will always check files brought in on removable media (such as CDs, flash drives etc) and mobile equipment (e.g., laptops, PDAs etc) with antivirus software and only use them if they are found to be clean of viruses. I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could damage files or software. I will only transport sensitive data on encrypted removable media (laptops, USB sticks etc).
- I agree to only using equipment within the context of my professional role;
  I will only use ICT equipment for [name of organisation] purposes. I understand that activities such as buying or selling goods are inappropriate.

Security and Privacy:
- I agree to take measures to protect access to data;
  I will keep my log-on user name and password private, always log off when I have finished working or am leaving the ICT equipment unattended and regularly change my password (minimum of every 3 months). I am aware that I must never use someone else’s user name. To protect myself and the systems, I will respect the security on the ICT equipment; I understand that attempting to bypass or alter the settings may put my work or other people’s information at risk. I will not send sensitive information via FAX or non-secure email.

Mobile phones:
- I agree to always abide by [name of organisation’s] policy for use of mobiles in the workplace;
  I understand that the use of mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of my line manager and recorded.

Name (print)…………………………………………………………………………………… Signed…………………………………………………

Organisation…………………………………………………………………………………… Date…………………………………………………………
2. Safety in a Digital World: Guide for Parents/Carers:

You were taught road safety,

You were taught rail safety,

You were taught to play safely.

In the 21st Century you and your children need to be taught e-safety

Children access the Internet on:

- Computers, PCs, laptops and tablets
- Mobile phones
- Games consoles
- Music systems, MP3 players and iPods.
- And they play games online with friends and strangers

They blog, chat, enter competitions, social network, email, watch TV online, download and upload information. They are creative at making music, making films and making web content.

Are you worried about their safety whilst accessing the internet?

This leaflet will provide you with some basic information to help you feel more confident in supporting your child to be e-safe.

The Benefits of Digital Technology

There are many benefits of having access to digital technologies. Here are some of them:

- Used effectively, these can improve children’s achievement.
- Using them at home and at school develops skills for life.
- Children with supportive and involved parents and carers do better at school.
- Children enjoy using them.
- Using technologies provides access to a wider and more flexible range of learning materials.

Staying Safe

You can make a huge difference if you talk to your child about how they use digital technology, let them know you are there to guide them and pass on essential safety advice. Here are some do’s and don’ts:

- Do keep your computer in a place where everyone can use it, go online with your child so you can see what they are doing on the internet.
- Do remind children that everyone they meet online for the first time is a stranger even though they might behave like a friend.
- Do encourage your child never to meet up with someone they make friends with online, if they do then make sure they take along a trusted adult and meet in a public place.
- Do explain to children that they shouldn’t accept emails or open files from people they don’t know. They may contain viruses, nasty messages or annoying links to things you don’t want them to see.
• Do be aware that your child may be a cyber-bully or a target of cyber-bullying. Be alert to your child seeming upset after using the internet or their mobile phone.
• Do talk to your child so they know they can come to you if they run into any problems. Your continued involvement is the best way of keeping your child safe.
• Do make clear what content and behaviour is acceptable and check that sites are age appropriate.
• Do give your child the knowledge and skills to build up resilience to the things they find online, help them to play and learn safely.
• Do use filtering software and agree ground rules about what services you are happy for your child to use.
• Do know how to complain to your Internet Service Provider (ISP).
• Don’t allow them to give out personal information. That means full name, home or school address, telephone number or personal email or mobile number.
• Don’t allow your child to access inappropriate sites.

If you want to find out more
A guide for parents about the potential dangers facing their children on the internet, plus advice on what parents can do to help counter these hazards: www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety

Find the latest information on web sites, mobiles and new technology. Find out what’s good, what’s not and what you can do about it: www.thinkyouknow.co.uk

The UK Council for Child Internet Safety (UKCCIS) brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Safer Children in a Digital World consultation: www.dcsf.gov.uk/ukccis

Childnet International is a non-profit organisation working with others to help make the Internet a great and safe place for children: www.childnet-int.org

The Child Exploitation and Online Protection Centre (CEOP) works across the UK tackling child sex abuse and providing advice for parents, young people and children about internet safety: www.ceop.gov.uk

Or call the Hull Educational IT Helpdesk: 01482 785240

Teach your child the internet safety code, Click Clever, Click Safe.

• **Zip It** – Keep your personal stuff private and think about what you say and do online.
• **Block It** – Block people who send you nasty messages and don’t open unknown links and attachments.
• **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.
3. Safety in a Digital World: Guide for Children and Young People:

Digital technology opens up a world of entertainment, opportunity and knowledge. To help you stay safe this guide aims to provide information on:

- The benefits of Digital Technology;
- Addressing the risks;
- Further advice and support.

The safety advice in this leaflet applies to all digital technology including computers, mobile phones, TVs, iPods, mass storage devices, tablets and laptops etc.

The Benefits of Digital Technology

You can use digital technology for many reasons, including:

Finding and sharing information – Researching topics on the internet, for school, college and for personal interests, and sharing media like files, pictures, films and music.

Keeping in touch with family and friends – Staying in touch with family and friends through Email, Instant Messaging (IM), Social Networking and chat rooms. Technology can be useful for contacting people in an emergency and making new friends in a safe way.

Entertainment – Listening to music, watching films, and playing interactive games.

Shopping – Buying items from companies and individuals all over the world, including online auctions.

Addressing the risks: Digital technology agreement:

There are some risks in using digital technology – follow this advice and sign this agreement to help keep you safe.

I agree to keep my personal information safe

Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings. This can help keep you safe.

Don’t give out personal information like email addresses, home or school addresses or mobile phone numbers to people you do not know.

Only post photographs which you would be happy with your parents/carers seeing and make sure they don’t show addresses. Photographs you post can be copied and sent to other people meaning you are not in control of them.

Do not share your passwords and log in details as people could access your information without your permission.
I agree not to access sites that are inappropriate for my age or download inappropriate content and I will tell adults about the sites that I am worried about.

Some sites include inappropriate content like pornography, violence, racism, sexism and gambling. It is not appropriate to access these sites.

I agree not to meet people without asking a parent/carer/adult.

Some people on the internet are not who they say they are. Be careful who you chat to and make friends with on Social Networking sites like Facebook, Twitter, Chat Roulette, Omegle, My Space, Bebo, Ask FM or Snapchat. Never agree to meet someone without telling an adult you trust.

I agree to report any worries I have to an adult.

If anyone online makes you worried or says things that make you feel uncomfortable tell an adult or click ‘Report abuse’ button (some websites will ask you to download this first) and block the person.

Do not respond to upsetting messages and cyber-bullying. Keep the message and show it to an adult you trust.

I agree not to send rude or pornographic pictures or videos (often called ‘sexting’).

By sending images of this type you could be committing an offence.

I agree not to use digital technology to bully people or make threats.

Cyberbullying is not acceptable and can cause distress.

Signed...........................................................             Date..................................

Further advice and support:

If you want to find out more about using digital technology safely go to:

www.thinkyouknow.co.uk  Digital safety advice
www.ceop.gov.uk  Report Abuse Button

Remember the internet safety code: Click Clever, Click Safe.

•  Zip It – Keep your personal stuff private and think about what you say and do online.
•  Block It – Block people who send you nasty messages and don’t open unknown links and attachments.
•  Flag It – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.
Response to an Incident of Concern:

An important element of e-safeguarding is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The organisation shall establish an incident reporting procedure and record reported incidents in an ‘Incident Log’. This log should capture the information contained in 2.4.8.

The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Senior Leadership Team/Senior Manager within the organisation at a minimum frequency of once per term or quarterly. Through this review process, where deemed appropriate, management shall update the risk assessment in light of new incidents. The Log and accompanying action plans should be reviewed annually by the Governing Body/Trustee.

Organisations could usefully draw up a list of common incidents from the log. For example:

Possible incidents:

- Circumventing the network security system and/or use of ‘proxy’ sites;
- Accessing, storing and/or disseminating inappropriate material (a definition of which should be in the AUP);
- Installing unapproved software;
- Using other people’s accounts, email addresses or passwords without permission;
- Breaching copyright;
- Uploading an organisation’s material onto a social network or chat room without permission;
- Leaving school mobile devices unattended;
- Not logging off when leaving a device.
E-incident Log Sheet:

E-incident Log Sheet 1 - member of staff identifying incident - front cover

<table>
<thead>
<tr>
<th>To be completed by the member of staff identifying the incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of identification:</td>
</tr>
<tr>
<td>Time of identification:</td>
</tr>
<tr>
<td>Duration of incident:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Description of the e-safety incident:
(please give as much information as you are able - use the prompts overleaf in the guidance)

Description of information recorded or secured
(please refer to legal guidance overleaf)

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have files, audio/text/images been recorded and secured?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has any computer or other technology including phones been secured?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If yes, how and where, who by and when?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What actions were taken, and by whom? Give details of agencies informed and contact person within those agencies.

Name of person completing this form:

Organisation:

Date: Signature:

Send this form immediately to the person with responsibility for child protection within your organisation
Version: Thursday, 17 April 2014

E-incident Log Sheet 1 – member of staff identifying incident – guidance overleaf

**Date and Time section:**
Please complete all sections, if you don’t know the exact day or time of the incident, please write 'unknown'

**Description of the e-safety incident:**
It is vital that all details you know are recorded, including how the information became known to you and from whom. If there is insufficient space on the form, please use additional sheets, but ensure that they are firmly attached and a note clearly identifies additional sheets used. Include detail of specific services or websites used if known (e.g., chat room, instant messenger); e-mail addresses; usernames etc. Give full details of real names and e-mail addresses etc where known. Some prompts to assist you could be:
- How was the incident identified? Who was involved and how do you know this? Why do you have concerns?

**Description of information recorded or secured**
Legal guidance for those reporting E–SAFETY incidents that involve a criminal offence

**POWERS**

If any person has reasonable grounds to believe that an offence IS being committed, then they may detain the person (offender only) if safe to do so and secure any evidence of the offence (including property). This would include the property of a victim or offender.

Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

**Offences committed via computers/laptops/mobile phones.**
In these situations the securing of information must be carried out in a specific way in order to obtain the best evidence possible for the police and other law enforcement agencies.

When a computer is turned on or on standby it should be left exactly as it is; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to record in note form any details that can be seen on the screen. DO NOT follow any links or change any pages.

Information that should be noted if on screen
- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information
- Any text from chat conversations.

If inappropriate behaviour is conducted via any device or website like MSN, FACEBOOK, any 'chat' forum or social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured).

This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.

The above information is not an exhaustive list and any other information noted on screen should be included.

**Actions taken**
Please give full details of other agencies that have been informed. If the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond ‘grooming’ and may be linked to other criminal activity. This may include racist incidents, extremist radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list. The form must then be signed and dated and handed as soon as possible to the person responsible for child protection within your organisation.
E-incident Log Sheet 2 - Notifications and Actions - person with responsibility for child protection

To be completed by the person with responsibility for child protection within the organisation

<table>
<thead>
<tr>
<th>Notifications:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Was notification to the Local Authority Designated Officer required?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. If yes, what was the outcome?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Have you notified the police?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Please give details with reference to guidance overleaf.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NB This is not an exhaustive list there may be other actions you are required to carry out within your specific organisation.

Conclusion to the incident:

<table>
<thead>
<tr>
<th>Have specific vulnerabilities or trends been identified?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>If yes, what action will now be taken?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name of person completing this form:

Organisation:

Date:                       Signature:
E-incident Log Sheet 2 – person with responsibility for child protection – guidance overleaf:

**Notifications**
Please give full details of other agencies that have been informed. The person initially identifying the incident may have already contacted others, please also record them here, plus any additional action taken by you after receiving the completed Log Sheet 1.

As with Log Sheet 1, if the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond ‘grooming’ and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list.

It is possible that information has not been recorded and secured by the member of staff completing Log Sheet 1. You are reminded that you have powers to detain and secure if you have reasonable grounds to believe that an offence IS being committed. You may detain the person (offender only) if safe to do so and secure any evidence of the offence (including property). This would include the property of a victim or offender.

Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

**Offences committed via computers/laptops/tablets/mobile phones.**
In these situations the securing of information must be carried out in a specific way in order to obtain the best evidence possible for the police and other law enforcement agencies.

When a computer is turned on or on standby it should be left exactly as it is; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to record in note form any details that can be seen on the screen. DO NOT follow any links or change any pages.

Information that should be noted if on screen
- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information
- Any text from chat conversations.

If inappropriate behaviour is conducted via any device or website like on MSN, FACEBOOK, any ’chat’ forum or Social networking site. DO NOT DELETE or interfere with the offending account, (this will be done when the evidence is secured).

This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.

The above information is not an exhaustive list and any other information noted on screen should be included.

**Conclusion to the incident**
Please record any disciplinary action taken or communications with parents/carers or other agencies, as well as specific detail of future meetings, monitoring or discussion planned.

**Vulnerabilities and Trends**
If there are additional vulnerabilities and trends that have been revealed by the incident, there may be a need to review organisational policy or pass information to other agencies at a later date, either once the investigation has been concluded or even before that.

Please record all details that you are able to provide at this stage.

**Name, organisation and date**
Please complete and sign Log Sheet 2 and retain in a secure location for monitoring purposes.
Response to Risk Flowchart

Response to and Reporting of an E-safety Incident of Concern

If a child is at immediate risk

Consult with Children’s Social Care (CSC)

Contact police (999) urgently if there is immediate danger

E-safety incident occurs

Illegal Activity or Material found or suspected

Content

Activity

Contact e-safety officer and/or CSC

Report to Internet Watch Foundation (www.iwf.org.uk) and/or Police

Report to Police and CEOP www.ceop.police.uk

Staff allegations procedures and/or criminal action

Child protection procedures and/or criminal action

Possible Actions:
• Inform e-safety officer
• Follow child protection procedures
• Sanctions
• PSHE/Citizenship
• Anti-bullying
• Parental work
• Support e.g., counselling, peer mentoring

Inappropriate Activity or Material

Activity

Content

Contact e-safety Officer and/or CSC

Possible Actions:
• Inform e-safety officer
• Follow staff allegations procedures
• Disciplinary action
• Staff training
• Support e.g., counselling

Staff

Child

Report to filtering manager and/or organisations Broadband helpdesk.

If necessary follow possible actions under inappropriate Activity

Contacts
• Hull Children’s Social Care (CSC): 448879.
  Emergency Duty Team: 788080
• East Riding Children’s Social Care (CSC): 396840
  Emergency Duty Team: 880826
• Police: 0845 6060222 (999 in emergency circumstances)
• Safeguarding Children Boards:
  Hull: 846082
  East Riding: 396998/9
• Child Exploitation and Online Protection Centre (CEOP):
  www.ceop.police.uk

Record actions in e-safety Incident log sheet (ensure kept in secure place), review e-safety policies and procedures; implement any changes for the future
Communications:

What should the communications plan contain?
(\textbf{Name of organisation}) \textit{shall} include appropriate communications and/or training for all sectors of the organisation’s community.

This should cover:

- Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.
- Workforce training in responsible approaches to data on fixed or mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.
- A comprehensive and developmental e-safety curriculum for children and young people referenced in schemes of work and programmes of study in schools.
- The programme \textbf{should} include the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying and ‘sexting’.
- Regularly re-visiting of the AUP with staff and pupils.
- ICT non-teaching staff training related to how digital technology can enhance learning and teaching (see Becta’s FITS Foundation).
- Organisations \textbf{shall} create working Acceptable Use Policies (AUPs) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the organisational community. This policy \textbf{shall} be subject to annual review by the governing body/Trustee.

Organisations like ChildNet, ThinkyouKnow, CEOP, RM offer support for education and training materials.

How will the policy be introduced to children and young people?

Many children and young people are very familiar with fixed and/or mobile technology and Internet use and culture; it is therefore wise to involve them in designing the organisation’s Acceptable Use Policy on Safety in a Digital World and e-safety rules. As children and young people’s perceptions of the risks will vary; the e–safety rules may need to be explained or discussed.

HCC has produced resources available to display in organisations to remind children and young people of e-safety at the point of use.

The children, young people and parent/carer agreement should be attached to a copy of the organisation’s e–safety AUPs appropriate to the age of the pupil.

Consideration must be given as to the curriculum place for teaching e–safety; it could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever children and
young people are using the internet. E-safety must be a consideration for any organisation facilitating children and young people’s use of the internet.

A useful checklist could include:-

- Every child to be informed that network and Internet use will be monitored.
- Children and young people’s instruction in responsible and safe use should precede Internet access.
- An e–safety module should be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Safe and responsible use of the internet and technology is reinforced across the curriculum.
- Particular attention to be given where children and young people are considered to be vulnerable.
- Opportunities for confidential discussions and pastoral support to supplement the planned curriculum.

Useful e–safety curriculum resources and programmes include:

- ThinkUKnow: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Safe Social Networking: www.safesocialnetworking.com
- Safeguarding Children a Shared Responsibility – Awareness, Recognition and Responses (Level 1) http://www.hullchildrenstrust.org/
- E-safety Awareness: Safeguarding Children in a Digital World (Level 1) http://www.hullchildrenstrust.org/

How will the policy be discussed with staff?

It is important that all staff/volunteers feel confident to use new technologies in teaching and facilitating access to the internet for children and young people; the organisation’s e–safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for employees are specific and instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT use within their organisation, they should discuss this with their line manager to avoid any possible misunderstanding.
Particular consideration must be given when staff are provided with devices by the organisation which may be accessed outside of the organisational network. Organisations must be clear about the safe and appropriate use of organisationally provided equipment and rules about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of the organisation’s information.

All staff within (name of organisation) including administration, governors and volunteers shall be included in awareness raising and training. Induction of new staff/volunteers shall include a discussion of the organisation’s e–safety Policy.

- The e–safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff, children and young people, the organisation will implement Acceptable Use Policies.
- 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 the Senior Manager/ Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

How will parents’/carers’ support be enlisted?

Internet use in children and young people’s homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents/carers are aware of the dangers, children and young people may have unrestricted and unsupervised access to the Internet in the home. An organisation may be able to help parents/carers plan appropriate supervised use of the Internet at home and educate them on the risks. Parents/carers should also be advised to check if their child’s use elsewhere in the community is covered by an Acceptable Use Policy. One strategy is to help parents/carers to understand more about ICT — perhaps by running parent/carer awareness sessions.

- Parents’/carers’ attention will be drawn to (name of organisation) e-safety Policy in newsletters, the brochure and on the (name of organisation) website as well as through the organisation’s Child Protection Policy and Procedures.
- A partnership approach with parents/carers will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–safety at other attended events e.g. sports days.
- Parents/carers will be requested to sign an e–safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents/carers on e–safety will be made available to parents/carers in a variety of formats.
- Advice on filtering systems, educational and leisure activities that include responsible use of the Internet will be made available to parents/carers.
- Interested parents/carers will be referred to organisations listed in section 4.3.
Organisational Roles:

Who will write and review the policies?
Overall responsibility for e-safeguarding rests with the Senior Leadership of an organisation. However, e-safeguarding is everyone’s responsibility, whether they are a member of staff/employee/volunteer, a child or young person, parent/carer or a governor/trustee. Failure to apply agreed controls to secure data and e-safety can be a serious matter, and the e-safeguarding procedures outlined in this guidance assume the designation of named staff to specific roles.

The e-safety policy should relate to other policies including those for safeguarding and child protection, ICT, behaviour, anti-bullying, and in education the personal, social and health education (PSHE) and citizenship. Policy construction provides an opportunity to review practice and the more that staff, parents/carers, governors, children and young people are involved in deciding the policy, the more effective it will be.

The organisation should appoint an E-safety Co-ordinator (or equivalent). This may be the Designated Child Protection Co-ordinator as the roles overlap.

The E-safety Co-ordinator should be a senior member of staff who is familiar with the risks and the organisation’s response. Typically, the E-safety Co-ordinator has the following responsibilities;

a) They own the e-safety and e-security policies, including risk assessment.
b) They keep a record of all staff responsible for compiling and retaining specific information.
c) They act as an advocate for e-safety and e-security.

How are the policies reviewed in organisations within Hull?

Hull Safeguarding Children Board e-safety work-stream will ensure:
- The Hull E-safety Toolkit is reviewed by the e-safety work-stream.
- Any changes and additions shall be circulated to all those adopting the Toolkit.
- The electronic version of the Hull E-safety Toolkit is kept up to date to ensure its currency. In addition, the e-safety work-stream will provide updates regarding new and emerging technologies and e-safety issues via the HSCB website.

The HSCB e-safety work-stream will offer support and advice to all organisations in their adoption and implementation of the Hull E-safety Toolkit.

Education and Training:

The CEOP Ambassador training course enables professionals to train fellow professionals in the delivery of CEOP’s ‘Thinkuknow’ education programme.

CEOP Ambassadors are trained with an in-depth look at how young people use the internet and mobile technology. They also know how offenders use the online environment to groom children.

The CEOP Thinkuknow training course enables professionals to deliver CEOP’s Thinkuknow programme directly to young people. As well as teaching how to deliver the resources the training
course also takes participants through some of the most popular applications used by young people in the online and mobile environment.

The organisation’s E-safety Co-ordinator (see 3.2.1) has a vital role that requires regular and up-to-date professional development. HSCB recommend that the E-safety Co-ordinator undergoes an appropriate level of training, including:-

**Child Exploitation Online Protection Training:**

- CEOP Thinkuknow training
- CEOP Ambassador training

**Hull Safeguarding Children Board Training:**

- Safeguarding Children – A Shared Responsibility (Level 1)
- E-safety Awareness – Safeguarding Children in a Digital World
- Exploring the Impact of Child Sexual Abuse
- Child Sexual Exploitation
- Safeguarding Disabled Children
- Domestic Violence

Those E-safety Co-ordinators who are also Child Protection Co-ordinators must have completed the required training for this role.

Please note this is not an exhaustive list of training, a range of courses are available in the HSCB Safeguarding Training Programme. This is available either by contacting the Partnership Learning Centre on 318949 or via the following web link: [http://www.hullchildrenstrust.org/](http://www.hullchildrenstrust.org/)
E-Safety Audit:
This self-audit should be completed by the member of the Senior Leadership Team/Senior Manager responsible for e–safety policy. Many staff could contribute to the audit including: Designated Child Protection Co-ordinator, E-safety Co-ordinator, Network Manager and in school include and Head teacher.

<table>
<thead>
<tr>
<th>Please insert the necessary details in the rows below or tick Yes/No as appropriate:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the <em>(name of organisation)</em> got an e–safety Policy that complies with HCC guidance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of latest update (at least annual):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The <em>(Name of organisation)</em> e–safety policy was agreed by governors/trustees on:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The policy is available for staff/volunteers at:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The policy is available for parents/carers at:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The responsible member of the Senior Leadership Team/Senior Manager is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The responsible member of the Governing Body is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Designated Child Protection Co-ordinator is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The E–safety Co-ordinator is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has e–safety training been provided for all children and young people (age appropriate) and all members of staff?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a clear procedure for a response to an incident of concern?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have e–safety materials from CEOP, Childnet and Becta been obtained?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do all staff/volunteers sign a Code of Conduct or Acceptable Use Policy on appointment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all children and young people aware of the e–safety rules or Acceptable Use Policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are e–safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all children and young people?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do parents/carers sign and return an agreement that their child will comply with the School e–safety rules?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are staff/volunteers, children and young people, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has an ICT security audit been initiated by Senior Leadership Team/Senior Manager, possibly using external expertise?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is personal data collected, stored and used according to the principles of the Data Protection Act?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Internet access provided by an approved educational Internet service provider which complies with DFE requirements <em>(e.g. YHGFL, Regional Broadband Consortium, NEN Network)</em>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the organisational-level filtering been designed to reflect educational objectives and approved by Senior Leadership Team/Senior Manager?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of the Senior Leadership Team/Senior Manager?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have appropriate teaching and/or technical members of staff attended training on the YHGFL filtering system?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version: Thursday, 17 April 2014
Managing Technology and Access:

Managing Information Services:

How will information systems security be maintained?
It is important to review the security of the whole system from user to Internet Service Provider. This is a major responsibility that includes not only the delivery of essential services but also the personal safety of staff, children and young people.

Data security is a complex matter and cannot be dealt with fully in this document. However, the person in charge of data security needs to be identified within the organisation; this could be a network manager, business manager, or technical manager. Note the role is distinct and separate from the ‘E-safety co-ordinator’, a role identified in 3.2.1.

All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation and for HCC.

Local Area Network (LAN) security issues include:
Possible statements:

- Access to all ICT systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the person in charge of data security. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where ‘restricted’ information is stored, access shall only be granted to individuals approved by the person in charge of data security. A record shall be kept of these approvals.
- All access controls should be reviewed each term, to ensure that any users that leave the organisation have their access removed.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For HCC staff, flouting the electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes that compromise access or security and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and must be password protected e.g. password changed daily to control anonymous access and only given out on request.
- Portable media may not be used without specific permission followed by a virus check.
• Unapproved software will not be allowed in pupils’/staff work areas or attached to email.
• Files held on the organisation’s network will be regularly checked.
• The person in charge of network management will review system capacity regularly.

Wide Area Network (WAN) security issues:
Possible statements:

• Where any external network traffic is allowed from the Internet to the organisation, a local firewall shall be deployed to restrict traffic to only necessary ports and IP addresses.
• Where the organisation’s external Internet connection allows connections from other organisation’s behind a shared firewall, a local firewall should be considered to restrict this traffic.
• All Internet-facing systems shall be placed onto a separate network segment; a de-militarised zone (DMZ), with access to applicable services, controlled by a firewall.
• Where externally facing services may be at particular risk, the addition of an Intrusion Prevention System (IPS) should be considered.
• The use of external specialist third-party penetration testing should be considered on an annual basis for Internet visible systems.
• All wireless implementations shall be a minimum of WPA 2 encryption, and shall require authentication prior to connection. Where possible, wireless networks should be further restricted through the firewall.
• The use of shared folders on workstations and laptops should be discouraged. If used ensure folders are password protected.
• All Internet connections must be arranged via Hull CC, RM or Hull CLC to ensure compliance with the security policy.
• Personal data sent over the Internet or taken off site will be encrypted.
• The security of the (name of organisation) information systems and users will be reviewed regularly, at least annually.

How will filtering be managed?
Levels of Internet access and supervision will vary according to the child or young person’s age and experience. Access profiles must be appropriate for all members of the organisation. Older young people, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism, radicalisation, harassment, or Sex and Relationship Education (SRE). In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

Possible statements:

• Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
• A walled-garden or “allow-list” restricts access to a list of approved sites. Such lists inevitably limit children and young people’s access to a narrow range of information.
• Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
• Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
• Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
• Key loggers record all text sent by a workstation and analyse it for patterns. False positives will require manual checking.

Organisations installing their own filtering systems are taking on a great deal of responsibility and demand on management time. Hundreds of inappropriate sites are created each day and many change URLs to bypass filtering systems.

Possible statements:

• The (name of organisation) will work with HCC, RM or YHGfL team to ensure that systems to protect children and young people are reviewed and improved.
• If adults or children and young people discover unsuitable sites, the URL must be reported to the E–safety Co-ordinator, a named person in the organisation.
• The organisation’s broadband access will include filtering appropriate to the age and maturity of children and young people.
• Larger schools, generally secondary, may manage the configuration of their filtering. This task requires both educational and technical experience.
• A senior member of staff in the organisation will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
• Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children’s Social Care, IWF or CEOP. See Response to Risk Flowchart.
• The organisation’s access strategy will be designed to suit the age and requirements of the children and young people, with advice from network managers.

How will videoconferencing be managed?
Videoconferencing enables users to see and hear each other between different locations and uses a number of applications including FaceTime and Skype. This ‘real time’ interactive technology has many uses in educational settings. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety — you can see who you are talking to — but if inappropriately used, a video link could reveal security details.

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures.

The National Educational Network (NEN) is a private broadband, IP network interconnecting the ten regional schools’ networks across England with the Welsh, Scottish and the Northern Ireland networks.
Schools with full broadband are connected through the YHGfL and have access to services such as gatekeepers and gateways to enable schools to communicate with external locations.

Conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part. Check who has signed into your conference; as a guest without a camera would not be visible.

**The equipment and network**

- All videoconferencing equipment must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- Videoconferencing equipment should not be taken off (name of organisation) premises without permission.

**Users**

- Children and young people should ask permission from the supervising member of staff before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the young person’s age.
- Parents and carers should agree for their children to take part in videoconferences, probably in the annual return.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the videoconferencing services should only be issued to members of staff and kept secure.

**Content**

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

**How can 'emerging technologies' be managed?**

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, collaboration and multimedia tools. Users can be mobile using a phone, games console or personal digital assistant or tablet with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as children and young people using a phone to video a person’s reaction in a difficult situation. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established.
Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

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

Organisations should keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. For instance, text messaging via mobile phones is a frequent activity for many children, young people and families; this could be used to communicate a pupil’s absence or send reminders for exam coursework. There are dangers for employees/volunteers however if personal phones are used to contact children and young people and therefore an organisationally owned phone should be issued. The policy needs to be carefully constructed so that it does not contradict or limit the appropriate educational use of other electronic personal devices.

The inclusion of inappropriate language, images and/or videos is difficult for adults to detect. Children and young people may need reminding that such use is inappropriate and conflicts with the organisational policy. Abusive messages should be dealt with under the organisation’s behaviour and/or anti-bullying policies.

Possible statements:

- The organisation should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on mobile phone use in the organisation.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the organisation is allowed.
- Staff will be issued with an organisation mobile phone where contact with children and young people is required.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.

How will Learning Platforms and VLEs be managed?
An effective learning platform or virtual learning environment can offer organisations a wide range of benefits to staff/volunteers, children and young people, parents/carers as well as support management and administration. It can enable children, young people and staff to collaborate in and across organisations, can share resources and tools for a range of topics, create and manage digital content and develop online and secure e-portfolios.

The Learning Platform/Environment (LP) must be used subject to careful monitoring by Senior Leadership Team/Senior Manager. As the usage grows, then more issues could arise regarding content, inappropriate use and behaviour online by users. The Senior Leadership Team/Senior Manager has a duty to review and update the policy regarding the use of the Learning Platform annually and all users must be informed of any changes made.
Advice from Becta: http://www.becta.org.uk/makelearningpersonal.php

Possible statements:

- Senior Leadership Team/Senior Manager and staff/volunteers will monitor the usage of the LP by children, young people and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Children and young people/staff/volunteers will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, children and young people etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of Senior Leadership Team/Senior Manager before reinstatement.
  e) A pupil’s parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the Senior Leadership Team/Senior Manager. In this instance there may be an agreed focus or a limited time slot.
- Children and young people may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Privacy and Protection:

How should personal data be protected?
The quantity and variety of data held on children and young people, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner’s Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:
Organisations will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Hull City Council Data Protection information may be seen at www.hullcc.gov.uk.

Password security:

Passwords are an important aspect of information security, and are the usual way to protect access to information. As such, all members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords.

These steps should include:

Possible statements:

- Keeping their password secure from others.
- Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£$%^) can help.
- Changing passwords regularly e.g. every three months.
- Staff/volunteers should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- In addition, when leaving a computer for any length of time, all staff members/volunteers shall log off or lock the computer, using CTRL+ALT+DELETE or other system command.
- Ensuring that there is a limit on the number of consecutive failed log in attempts. (Best practice is between 3 and 5 attempts)
- Restrict concurrent access i.e. a user should not be able to log in at the same time from two different machines, unless a generic or group login is appropriate.

How will email be managed?

The implications of email use for the (name of organisation) by children and young people need to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to children and young people that bypass the traditional (name of organisation) boundaries.

A central question is the degree of responsibility that can be delegated to individual children and young people as once email is available it is difficult to control. However, restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.
In the organisational context, email should not be considered private and most organisations reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of children and young people and the preservation of human rights, both of which are covered by recent legislation.

The use of email identities such as john.smith@hullschool.sch.uk generally needs to be avoided by children and young people, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify children and young people e.g., full name and their school/organisation. Secondary schools should limit pupils to email accounts approved and managed by the school. Protocols approved by BSF project in Hull are:

- Students: initial.surname@......
- Parents: initial-surname@......
- Staff: surname. initial@

For primary schools, whole-class or project email addresses should be used.

Possible statements:

- Children and young people may only use approved email accounts.
- Children and young people must immediately tell an adult if they receive offensive email.
- Children and young people must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Access in school/organisation to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and should be restricted.
- Email sent to external organisations should be written carefully and, if it contains potentially contentious information, authorisation should be sought before sending, in the same way as a letter written on school/organisation headed paper.
- The forwarding of chain messages is not permitted.
- Schools/organisations may have a dedicated email for reporting well being and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team/Senior Manager.
- Employee/volunteers should only use school/organisation email accounts to communicate with children and young people as approved by the Senior Leadership Team/Senior Manager.
- Employee/volunteers should not use personal email accounts during school/organisation hours or for professional purposes.

How will complaints be handled?

Parents, staff, children and young people should know how to use the organisation’s complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside the organisation. A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions will be required, linked to the organisation’s disciplinary policy. Potential child protection and illegal issues must be referred to the organisation’s Designated Child Protection Co-ordinator and/or E–

Possible statements:

- Complaints of Internet misuse will be dealt with under (name of organisation) Complaints Procedure.
- Any complaint about staff misuse must be referred to the E-safety Co-ordinator.
- All e–safety complaints and incidents will be recorded by (name of organisation) — including any actions taken.
- Children and young people and parents/carers will be informed of the complaints procedure.
- Parents/carers, children and young people will work in partnership with (name of organisation) to resolve issues.
- Discussions shall be held with/between (name of organisation), Children’s Social Care, Police and Hull Safeguarding Children Board to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to (name of organisation) disciplinary and child protection procedures.

How will published content be managed?
Excellent websites can inspire children and young people to publish work of a high standard. Websites can celebrate children and young people’s work, promote (name of organisation) and publish resources for projects.

Sensitive information about (name of organisation) and children and young people could be found in a newsletter but (name of organisation) website is more widely available. Publication of information should be considered from a personal and (name of organisation) security viewpoint. Material such as employee/volunteer lists or a plan may be better published in a handbook or on a secure part of the website which requires password authentication.

Possible statements:
- The contact details on the website should be the (name of organisation) address, email and telephone number. Employee/volunteer or children and young people’s personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. consider replacing ‘@’ with ‘AT’).
- The appointed senior leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with (name of organisation) guidelines for publications including respect for intellectual property rights and copyright.

Can pupil images and work be published?
The security of employee/volunteers and children and young people is paramount, the online publishing of children and young people’s names with their images is not acceptable as managing
the further use of published images is problematic. Published images could be re-used, particularly if large images of individual children and young people are shown.

‘Over the shoulder’ can replace ‘passport-style’ photographs but still convey the organisational activity. Personal photographs can be replaced with self-portraits or images of children and young people’s work or of a team activity. Children and young people in photographs should, of course, be appropriately clothed.

Images of children and young people should not be published without the parent’s or carer’s written permission. Some organisations ask permission to publish images of work or appropriate personal photographs on entry, some once per year, others at the time of use (this is an organisational decision).

Possible statements:

• Children and young people’s full names will not be used anywhere on the website, particularly in association with photographs and/or videos.
• Written permission from parents or carers will be obtained before images of children and young people are electronically published.
• Children and young people’s work can only be published with their permission or the permission of the parent/carer.

How will children and young people learn how to evaluate content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. In schools a whole curriculum approach may be required.

Policies need to empower children and young people to evaluate content critically and facilitate them in bringing to the attention of an adult any inappropriate content.

Possible statements:

• Children and young people should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
• The evaluation of on-line materials is a part of teaching/learning in every subject.
Legal Framework:

Notes on the legal framework
This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

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

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools may already have a copy of “Children and Families: Safer from Sexual Crime” a document published by the Home Office Communications Directorate.

More information about the 2003 Act can be found at [www.teachernet.gov.uk](http://www.teachernet.gov.uk)

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Data Protection Act 1998**
The Act requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing. Further details available at [www.ico.gov.uk/for_organisations/data_protection.aspx](http://www.ico.gov.uk/for_organisations/data_protection.aspx).

**The Computer Misuse Act 1990 (sections 1 — 3)**
Regardless of an individual’s motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else’s password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

**Malicious Communications Act 1988 (section 1)**
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

**Copyright, Design and Patents Act 1988**
Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
Further guidance given at www.copyrightservice.co.uk/copyright/p01_uk_copyright_law and www.hps.cam.ac.uk/students/plagiarism.html

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Protection from Harassment Act 1997
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess “extreme pornographic image”
63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”
Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of children and young people off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.
Useful Links & Contacts:
CEOP (Child Exploitation and Online Protection Centre)
www.ceop.police.uk

Childline
www.childline.org.uk

Childnet
www.childnet.com

Evaluating Online Educational Materials
http://www.libraryinstruction.com/evaluating.html

Hull Safeguarding Children Board (HSCB)
http://www.hullcc.gov.uk/portal/page?_pageid=296,1&_dad=portal&_schema=PORTAL
01482 846082

HSCB Training & Development Officer
E-safety Training
James.sykes@hullcc.gov.uk
01482 318949

Click Clever Click Safe Campaign
http://clickcleverclicksafe.direct.gov.uk

Cybermentors
www.cybermentors.org.uk

Digizen
www.digizen.org.uk

Internet Watch Foundation
www.iwf.org.uk

ICT in Libraries – data validation
www.ictl.org.uk/U1O3CG/page_02.htm

Kidsmart
www.kidsmart.org.uk

The Free Dictionary – for terms needing definition
www.thefreedictionary.com

CEOP (Think U Know) website
www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse
www.virtualglobaltaskforce.com
Yorkshire and Humberside Grid for Learning
www.yhgfl.net

Insafe
http://www.saferinternet.org/

BBC Web Wise (Safety & Privacy)
http://www.bbc.co.uk/webwise/topics/safety-and-privacy/

Pan European Game Information (PEGI)
http://www.pegi.info/en/index/

NASUWT (Guidance on cyberbullying)
http://www.nasuwt.org.uk/Whatsnew/Campaigns/StopCyberbullying/index.htm

UNISON (Guidance on social networking)
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786
**Glossary of Terms:**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUP</td>
<td>Acceptable Use Police</td>
</tr>
<tr>
<td>CEOP</td>
<td>Child Exploitation Online Protection</td>
</tr>
<tr>
<td>DMZ</td>
<td>DeMilitarised Zone - an additional layer of network security</td>
</tr>
<tr>
<td>HCC</td>
<td>Hull City Council</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Internet Domain</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IWF</td>
<td>Internet Watch Foundation</td>
</tr>
<tr>
<td>LP</td>
<td>Learning Platform</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>NEN</td>
<td>National Educational Network</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>RM</td>
<td>RM is the ICT subcontractor for Hull BSF.</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus (slot where memory sticks are connected)</td>
</tr>
<tr>
<td>VLE</td>
<td>Virtual Learning Environment</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access – wireless network security</td>
</tr>
<tr>
<td>YHGfL</td>
<td>Yorkshire and Humberside Grid for Learning</td>
</tr>
</tbody>
</table>
Publicity Materials and other Resources

1. Resources for parents and professionals on using Facebook

The following Facebook guidance can be accessed via www.yhgfl.net

- A parent’s guide to Facebook.
  http://www.connectsafely.org/pdfs/fbparents.pdf

- YHGfL Parental advice on Facebook.
  http://www.yhgfl.net/content/download/4790/53067/file/YHGFL%20Parental%20advice%20on%20Facebook.pdf

- YHGfL Guide for professionals using Facebook.
  http://www.yhgfl.net/content/download/4860/54504/file/YHGfL%20Guide%20for%20professionals%20using%20Facebook.pdf

- YHGfL Teacher tips for using Facebook.
  http://www.yhgfl.net/content/download/4748/52545/file/YHGFL%20Teacher%20tips%20for%20using%20Facebook.pdf

- Common Facebook issues for schools and how to solve them.
  http://www.yhgfl.net/content/download/4789/53063/file/Common%20Facebook%20issues%20for%20schools.pdf

2. 360° Safe

360° Safe offers organisations the opportunity to gain a quality mark for their E-safety Toolkit.
To explore this option access the following website: http://www.appraisal360.co.uk/

3. Early Years E-safety Toolkit

The early year’s toolkit – Online Safety A Toolkit for Early Years Settings produced by Plymouth Safeguarding Children Board can be accessed via:
http://www.plymouth.gov.uk/early_years_toolkit.pdf
Acknowledgments

This E-Safety Toolkit has been devised drawing upon the work of the following organisations.

**Becta** [www.becta.org.uk/safeguarding](http://www.becta.org.uk/safeguarding)

To ensure the educational community benefits from being able to re-use Becta materials, Becta has now adopted the Open Government licence (OGL). This ensures that stakeholders and website visitors will be able to benefit from the resources open for re-use under this licence.

**Kent County Council** [www.kenttrustweb.org.uk?esafety](http://www.kenttrustweb.org.uk?esafety)

**Leicester County Council** [www.leics.gov.uk/index/leisure_tourism/libraries/children/cybersafe/](http://www.leics.gov.uk/index/leisure_tourism/libraries/children/cybersafe/)

**YHGfL** [www.yhgfl.net](http://www.yhgfl.net)