Version: 1.1-June 2011

HULL
Safeguarding Children Board

Safety in a Digital World Guidance and Acceptable Use Policies Template

An E-safety Toolkit

Yorkshire & Humber GRID FOR LEARNING

Version: 1.1-June 2011

Contents

Preface

"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]

[1] Dr Tanya Byron (2008) *Safer children in a Digital World: The Report of the Byron Review* www.dcsf.gov.uk/byronreview/actionplan

Introduction

1.1 An E-safety Strategy for Hull

The digital world our children and young people live in is a rapidly changing place. New technologies are creating fantastic, exciting opportunities in communication, in learning and in many aspects of daily life. For many adults these developments seem quite different from what we have seen before. This makes us naturally cautious about them. However, for young people they are a regular and familiar part of everyday life that is being enthusiastically embraced.

This gives those of us whose role it is to safeguard our children and young people new considerations, challenges and new responsibilities. We want them to flourish through the many benefits that the digital world can offer. Yet at the same time we must help them understand and make informed decisions about what information they seek and share, the way that they do this and who they do it with.

We are clear about this responsibility in Hull. Under the guidance of the Hull Safeguarding Children Board E-safety workstream 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 and avoid the pitfalls and dangers.

When working in a field as complex and fast changing as e-safety, we must personalise the support we provide so that each individual 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.

This is not always easy; the pace of change means that as adults we can be in danger of feeling out-of-touch with and confused by technologies that young people are using. However, the onus is on us to overcome these potential barriers and take a balanced, responsible view.

Under the Children Act 2004 Section 11 and the Education Act 2002 Section 175, all professionals have a duty to safeguard and promote the well being of all children. This duty of care to safeguard and promote the welfare of children and young people 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 wider community. This requires an integrated approach across schools and other establishments in Hull (herein after described as “organisations”) that regularly come into contact with young people.

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 schools and other learning establishments, parents, carers, pupils and other professional organisations coming into contact with children, to sign-up to the principles contained within this document, the policies underpinning it and to respond effectively to any incidents arising.

Paul Dyson.

Independent Chair, Hull Safeguarding Children Board

1.2 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.

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as 'Recipient'	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact Child as 'Participant'	Tracking Harvesting Personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct Child as 'Actor'	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

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

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 learners 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

1.3 What do we mean by e-safeguarding?

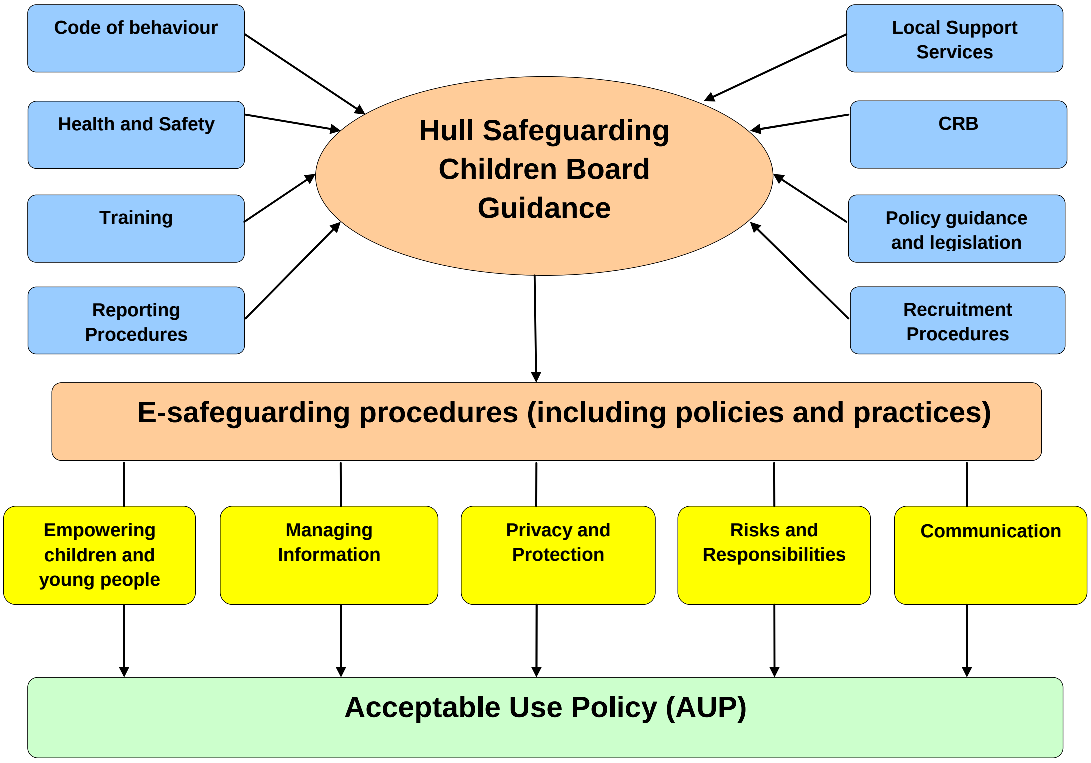
E-safeguarding procedures address all safeguarding issues which relate to the use of digital technology. There are two main elements to these issues:

1. E-safety
E-safety stands for 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 *etc*. 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.

1.4 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 and 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.


Code of behaviour
Health and Safety
Training
Reporting Procedures
Local Support Services
CRB
Policy guidance and legislation
Recruitment Procedures
Hull Safeguarding Children Board Guidance
E-safeguarding procedures (including policies and practices)
Empowering children and young people
Managing Information
Privacy and Protection
Risks and Responsibilities
Communication
Acceptable Use Policy (AUP)

1.5 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, organisational, network and data security 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 help and assistance in raising public awareness.

2.0 Guidance and Policy Template

This section of the **Hull E-safety Toolkit** provides a potential template that contains guidance and suggested statements for educational establishments and those providing services to children and young people 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, others to other services. It is important that individual institutions customise the guidance to provide clear documents, 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/ 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].

2.1 Empowering Children and Young People in the Digital World

2.1.1 Why is Internet use important?

The internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. With the growth of fixed and mobile technologies they now have faster, easier and more immediate access to online information than ever before (*e.g.,* laptops, personal digital assistants, webcams, digital video equipment, mobile phones, portable media players, e-readers and wireless internet access). Children and young people will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in **(name of organisation)** through digital technology.

Possible Statements:

- The Internet is a part of everyday life for education, business and social interaction. The **(name of organisation)** has a duty to provide children and young people with Internet access.
- Children and young people use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students/children and young people who show a responsible and mature approach to its use.
- The purpose of Internet use in **(name of organisation)** is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance the **(name of organisation)** management functions.

2.1.2 How does Internet use benefit children and young people?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

Benefits of using the Internet include:

Possible statements:

- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- exchange of curriculum and administration data with HCC and DfE;
- access to learning wherever and whenever convenient.

2.1.3 How can we ensure Internet use enhances learning and life experiences?

Increased computer numbers and improved Internet access may be provided but its impact on learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Children and young people need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

Possible statements:

- The **(name of organisation)** Internet access will be designed to enhance and extend education.
- Children and young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The **(name of organisation)** will ensure that the copying and subsequent use of Internet derived materials by staff, children and young people complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of children and young people.
- Staff should guide children and young people to on-line activities that will support the learning outcomes planned for their age and maturity.
- Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children and young people will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.1.4 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. Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy *etc* provide an opportunity for pupils to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

The extent to which the internet is used by extremists as a tool for radicalisation is not fully known , but it is clear that that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees.

The internet and social networking sites may provide a virtual online community to which a young person may wish to belong and then may in turn become increasingly exposed to extremism. Extremist websites may be used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for like minded individuals. The internet also offers easily accessible downloadable extremist material including advice and guidance on bomb making, filtered out of public systems, but often not at home – policies need to empower children and young people to evaluate content critically.

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.

2.2 Managing Information Services

2.2.1 How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning 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 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 eg. 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 include:
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.

2.2.2 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 or harassment. 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 confuse 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.

2.2.3 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. 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.

2.2.4 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 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 or images 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 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 phone where contact with children and young people is required.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.

2.3 Privacy and Protection

2.3.1 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:

- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual's rights;
- Kept secure; and
- Transferred only to other countries with suitable security measures.

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.

2.3.2 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+ATL+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.

2.3.3 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. 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@schoolname.hull4learning.net
Parents:	initial-surname@schoolname.hull4learning.net
Staff:	initialsurname@schoolname.hull.sch.uk or @schoolnameacademy.org.uk

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.

2.3.4 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 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.

2.3.5 Can pupil images and work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when children and young people can be included. Nevertheless the security of employee/volunteers and children and young people is paramount. Although common in newspapers, the publishing of children and young people's names with their images is not acceptable. Published images could be re-used, particularly if large images of individual children and young people are shown.

Strategies include using relatively small images of groups of children and young people and possibly even using images that do not show faces at all. "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.

Children and young people also need to be taught the reasons for caution in publishing personal information and images online.

Possible statements:

- Images that include children and young people will be selected carefully and will not provide material that could be reused.
- Children and young people's full names will not be used anywhere on the website, particularly in association with photographs.
- 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.

2.3.6 How will social networking and personal publishing be managed?

Parents/carers and professionals need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Children and young people should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All adults should be made aware of the potential risks of using social networking sites or personal publishing either professionally with children and young people or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. The internet and social networking sites may provide a virtual online community to which a young person may wish to belong and then may in turn become increasingly exposed to extremism.

Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

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. Examples would include 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 on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or young person or his/her location.
- Employee/volunteer official blogs or wikis should be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager. Employee/volunteer 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. Personal information must not be published 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.

ZIP IT
Keep your personal stuff private and think about what you say and do online.
BLOCK IT
Block people who send 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 offline.

2.4 Risks and Responses

2.4.1 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.
- 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.

2.4.2 How will risks be assessed?

E-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of digital technology is completely risk free. 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 and learning.

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.

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The 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 system. 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, 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.

2.4.3 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–safety Co-ordinator. Please refer to the Response to Risk Flowchart for reporting e-safety incidents.

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.

2.4.4 How should the Internet be used across the community?

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall and supermarket or cyber café. Ideally, children and young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access there is a fine balance to be achieved in ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and children and young people may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with children and young people on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance, filtering software should work across community languages and school Internet policies may need to reflect the children and young people's cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

Possible statements:

- The school will liaise with local organisations to establish a common approach to e–safety.
- The school will be sensitive to Internet related issues experienced by children and young people out of school, *e.g.,* social networking sites, and offer appropriate advice.

2.4.5 How will Cyberbullying be managed?

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

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that children, young people, organisations, and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people 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 cyberbullying: http://www.digizen.org/cyberbullying.

Possible statements:

- Cyberbullying (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 cyberbullying.
- All incidents of cyberbullying reported to **(name of organisation)** will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying:
  - ➢ 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 cyberbullying 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.

2.4.6 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://webarchive.nationalarchives.gov.uk/20101102103654/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.

2.4.7 Response to an Incident of Concern

An important element of e-safeguarding is the ability to identify and deal with incidents of concern and related to 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. 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 statements:

- Circumventing the network security system
- Accessing inappropriate material (definition should be in AUP)
- Installing unapproved software
- Using other people's accounts, email addresses or passwords
- Breaching copyright
- Uploading school material onto a social network or chat room
- Leaving school mobile devices unattended
- Not logging off when leaving a device

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.

CEOP REPORT
ceop.police.uk

2.4.8 e-Incident Log Sheet

e-Incident Log Sheet 1 – “member of staff identifying incident” – front cover

To be completed by the member of staff identifying the incident					
Date of identification:		Date of incident (if different):			
Time of identification:		Time of incident (if different):			
Duration of incident:		Do you know if repeat victim?	yes	no	unsure

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)**	Yes	No
Have files, audio/text/images been recorded and secured? Has any computer or other technology including phones been secured?		

If yes, how and where, who by and when?

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

e-Incident Log Sheet 1 – “member of staff identifying incident” – guidance

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)** 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 a request for inappropriate behaviour is made 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.

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, 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		
Notifications: 1. Was notification to the Local Authority Designated Officer required? 2. If yes, what was the outcome? 3. Have you notified the police? 4. Please give details with **reference to guidance overleaf**. **NB This is not an exhaustive list there may be other actions you are required to carry out within your specific organisation.**	Yes	No
Conclusion to the incident:		

Have specific vulnerabilities or trends been identified?	Yes	No
If yes, what action will now be taken?		

Name of person completing this form:			
Organisation:			
Date:		Signature:	

e-Incident Log Sheet 2 – "Notifications and Actions" - person with responsibility for child protection

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)** 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 a request for inappropriate behaviour is made 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 or carers, 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.

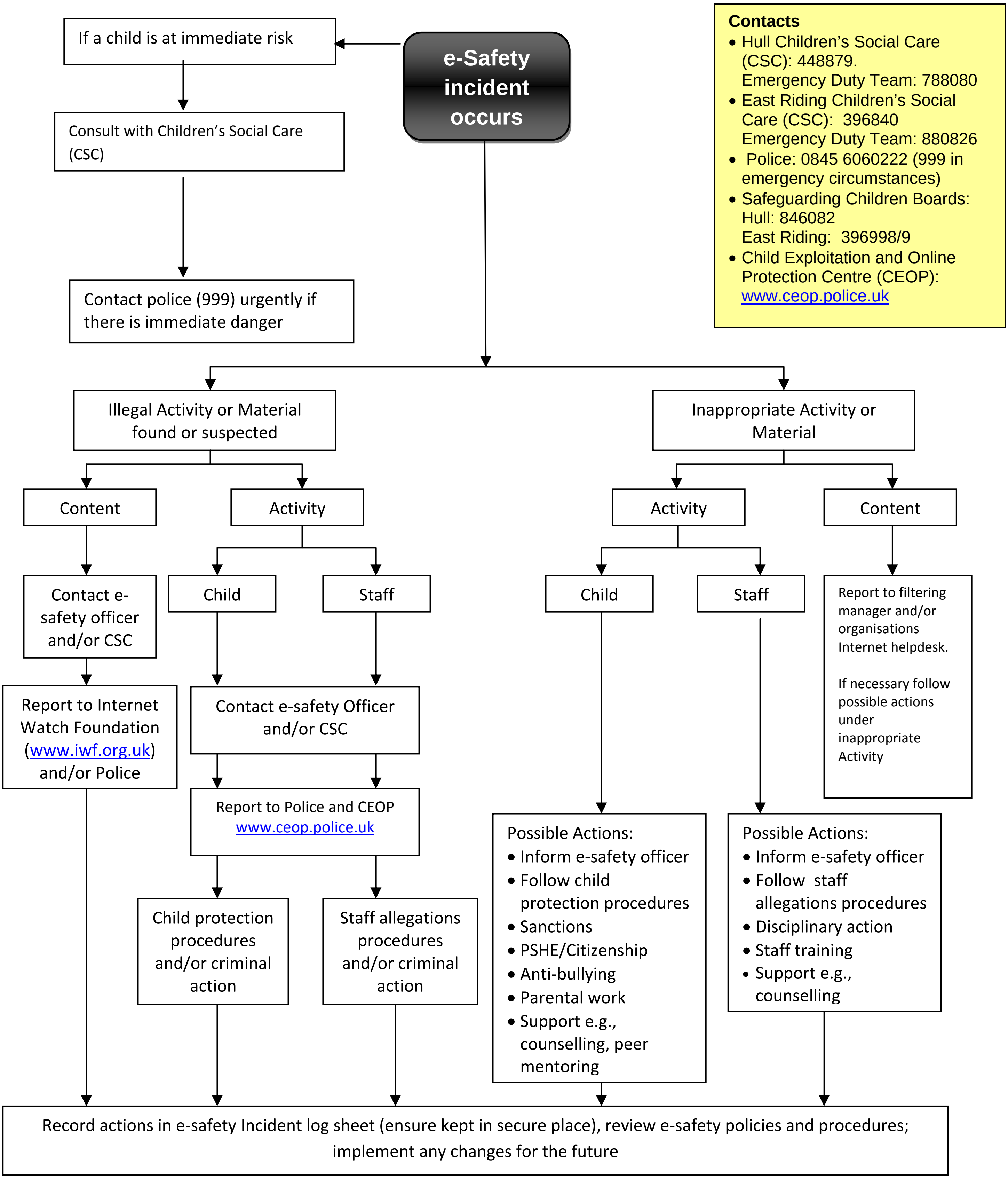
Please record all details that you are able to provide at this stage.

Name, organisation and date

Please complete and sign Log Sheet 2 and retain in a secure location for monitoring purposes.

2.4.9 Response to Risk Flowchart

Response to and Reporting of an e-Safety Incident of Concern



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

e-Safety incident occurs

If a child is at immediate risk

Consult with Children's Social Care (CSC)

Contact police (999) urgently if there is immediate danger

Illegal Activity or Material found or suspected

Content

Contact e-safety officer and/or CSC

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

Activity

Child

Staff

Contact e-safety Officer and/or CSC

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

Child protection procedures and/or criminal action

Staff allegations procedures and/or criminal action

Inappropriate Activity or Material

Activity

Child

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

Staff

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

Content

Report to filtering manager and/or organisations Internet helpdesk.

If necessary follow possible actions under inappropriate Activity

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

2.5 Communications

2.5.1 What should the communications plan contain?

(Name of organisation) ***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 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 **should** include the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying.
- □ 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.
- □ Organisations ***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 ***shall*** be subject to annual review by the governing body/Trustee.

Organisations like ChildNet, ThinkyouKnow, CEOP, Research Machines and Vital (http://vital.ac.uk/) offer support for education and training materials.

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

Many children and young people are very familiar with mobile and Internet use and culture and it is 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.

Hull City Council 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 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.

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 could 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) and Safeguarding Children in a Digital World (Level 1) http://www.hullchildrenstrust.org/
- E-safety Awareness: Resources for Parents, Professionals and Schools http://www.hullcc.gov.uk/portal/page?_pageid=296,671069&_dad=portal&_schema=PORTAL

2.5.3 How will the policy be discussed with staff?

It is important that all staff/volunteers feel confident to use new technologies in teaching and 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 teaching 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 HCC 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 organisational 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 Manger/ Team and have clear procedures for reporting issues.
- □ Staff training in safe and responsible Internet use both professionally and personally will be provided.

2.5.4 How will parents' 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. The school 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 appropriate use policy. One strategy is to help parents/carers to understand more about ICT — perhaps by running courses and parent 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 and 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.

3.0 Implementing Acceptable Use Policies

3.1 Development planning

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.

3.2 Organisational Roles

3.2.1 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 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 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.

3.2.2 How are the policies reviewed in organisations within Hull?

Hull Safeguarding Children Board e-safety workstream will ensure:

- The **Hull E–safety Toolkit** is reviewed by the e-safety workstream.
- 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 workstream will provide updates regarding new and emerging technologies and e-safety issues via the HSCB website.

The HSCB e-safety workstream will offer support and advice to all organisations in their adoption and implementation of the **Hull E-safety Toolkit**.
(http://www.hullcc.gov.uk/portal/page?_pageid=296,659697&_dad=portal&_schema=PORTAL)

3.3 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
- The Child Centred Approach – Understanding Children's Rights and Participation
- Exploring the Impact of Child Sexual Abuse
- 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/

3.4 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.

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

4.0 Appendices

4.1 Example AUPs

4.1.1 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……………………………………………….………………

4.1.2 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.

But now we are in the 21st Century and your children need to be taught e-safety

Children access the Internet on:

- **Computers**
- **Mobile phones**
- **Games consoles**
- **Music systems**
- **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 them that everyone they meet online is a stranger even though they might seem like a friend.
- Do encourage your child never to meet up with someone they make friends with online. But if they do then make sure they take along an adult you trust and to meet in a public place.
- Do explain 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 as likely be a cyberbully as be a target of cyberbullying. 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 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 consider using filtering software and agree ground rules about what services you are happy for your child to use.
- Do know how to complain.
- 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

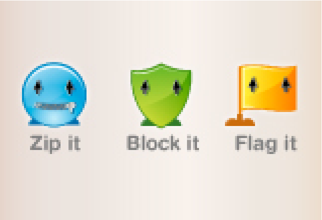
Childnet International is a non-profit organisation working with others to help make the Internet a great and safe place for children: www.childnet-int.org

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 01482 616719 for further help and guidance.

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.



4.1.3 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 *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 however 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, My Space or Bebo. Never agree to meet someone without letting an adult know.

I agree to report and 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 them.

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 films.

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......................................**

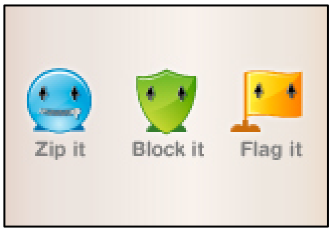
Further advice and support:

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.



4.2 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 whom 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.legislation.gov.uk/ukpga/2003/42/notes/contents

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.

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.hps.cam.ac.uk/students/plagiarism.html and www.copyrightservice.co.uk/copyright/p01_uk_copyright_law

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. 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.

Regulation of Investigatory Powers Act 2000

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.

4.3 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 City Council CYPS (Schools)
E-Safety Advice, Guidance and Support
mark.pinchbeck@hullcc.gov.uk
01482 616719

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

4.4 Glossary

Glossary of Terms

AUP	Acceptable Use Police
BSF	Building Schools for the Future project
CEOP	Child Exploitation Online Protection
DMZ	De-Militarised Zone - an additional layer of network security
HCC	Hull City Council
ICT	Information and Communication Technology
ID	Internet Domain
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IWF	Internet Watch Foundation
LP	Learning Platform
LAN	Local Area Network
NEN	National Educational Network
PC	Personal Computer
RM	RM is the ICT subcontractor for Hull BSF.
URL	Universal Resource Locator
USB	Universal Serial Bus (slot where memory sticks are connected)
VLE	Virtual Learning Environment
WAN	Wide Area Network
WPA2	Wifi Protected Access – wireless network security
YHGfL	Yorkshire and Humberside Grid for Learning

4.5 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 www.360safe.org.uk

3. Early Years E-safety Toolkit

The early years 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

5.0 Acknowledgments

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

Becta
http://webarchive.nationalarchives.gov.uk/20101102103654/nextgenerationlearning.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*

Leicester County Council *www.leics.gov.uk/index/leisure_tourism/libraries/children/cybersafe*

YHGfL *www.yhgfl.net*