National
Education
Network

e-Safeguarding:

Creating Working Procedures in Schools

Central Bedfordshire

Central Bedfordshire Council
and Bedford Borough Council

E2BN

YHGfL Yorkshire & Humber GRID FOR LEARNING

Acknowledgment to ECSC for guidance and support in the creation of elements of this manual

ecsc
more secure

Introduction

Rapidly developing information and communication technologies (ICT) are exciting and motivating learning tools through which learning and teaching can be greatly enhanced. This guidance provides a framework for schools to ensure ICT is used safely and responsibly and that risks related to ICT use is properly managed. The procedures outlined interpret the Becta guidelines and support the OFSTED safeguarding criteria. In the light of the implementation of these procedures, schools will need to consider how they will identify levels of compliance. This guidance refers to data held electronically, however the underlying principles of data security also apply to paper based data.

e-Safeguarding Procedures address all safeguarding issues which relate to the use of ICT. There are two main elements to these issues:

1. e-Security: Procedures to protect the physical network infrastructure to ensure all information and electronic data is securely maintained (see Risk Assessment below) and is categorised as **Public, Restricted or Protect** (see Information Classification below)

2. e-Safety: Procedures to ensure all members of the school community know their access rights and responsibilities in using ICT. These procedures are expressed in the school's Acceptable Use Policy (AUP).

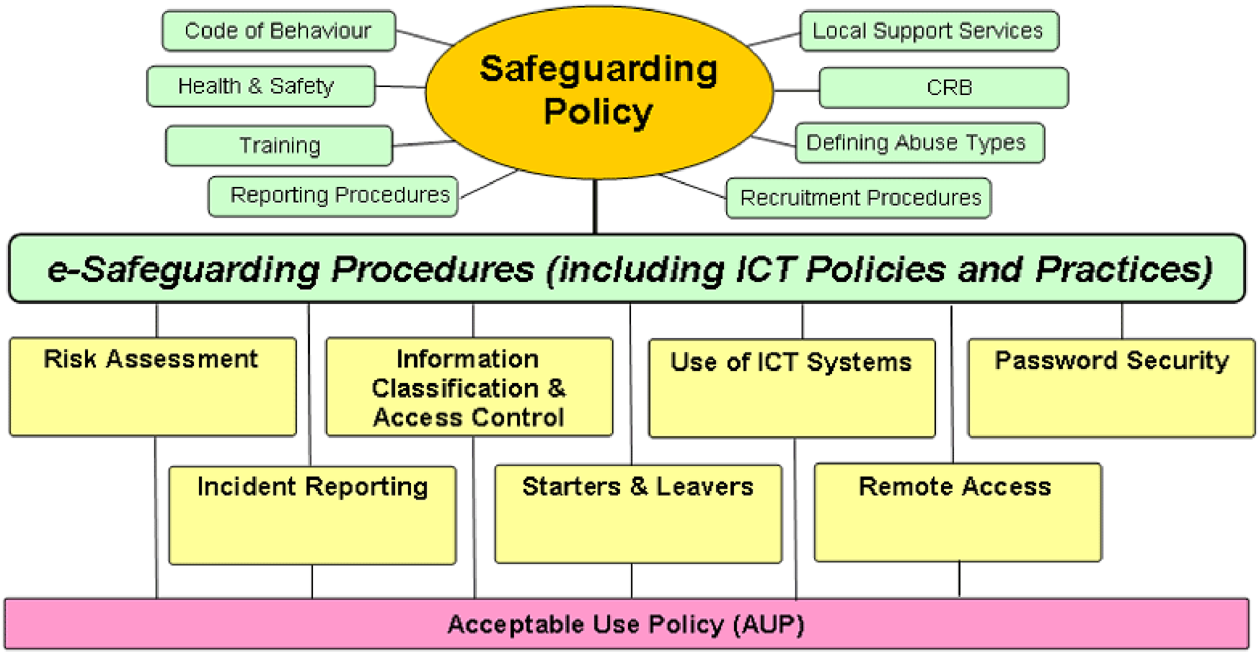
The purpose of this guidance is to highlight procedural areas of importance in e-safeguarding as part of the schools' Safeguarding Policy and to inform individual school's development of a working Acceptable Use Policy(s) (AUP).

Procedural requirements are expressed in two ways:

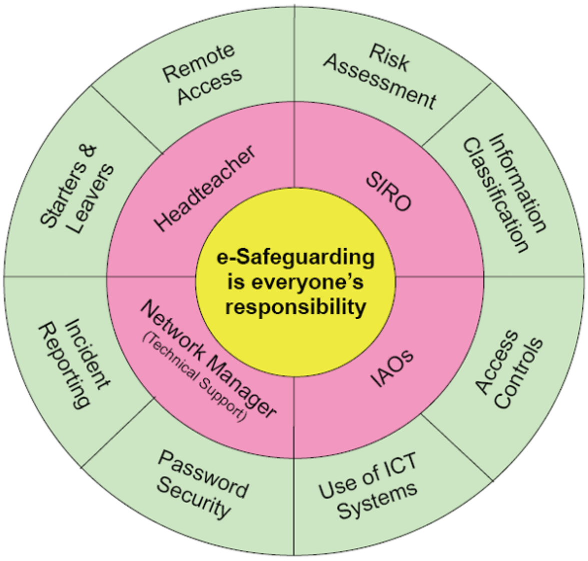
1. Mandatory elements: All statements with the word 'shall' are mandatory and are printed in bold italics. ***"Any identified non-compliance shall be reported as a risk to the Senior Information Risk Officer (SIRO)"*** (see 'roles and responsibilities' below) and have an action plan for compliance or be accepted by the Head Teacher.

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

In responding to these guidelines, schools 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 – an Acceptable Use Policy(s) (AUP).



Roles and Responsibilities



Although overall responsibility for e-Safeguarding rests with the Head Teacher and Governing Body, all e-Safeguarding procedures outlined in this guidance assume the designation of named staff to the following roles:

1. ***Senior Information Risk Officer (SIRO)*** is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the Senior Leadership Team and have the following responsibilities;

   a) They own the information risk policy and risk assessment
   b) They keep a record of all Information Asset Owners (IAOs) – see below
   c) They act as an advocate for information risk management
   The SIRO should never be the Network Manager; the Network Manager implements decisions made by the SIRO.

2. ***Information Asset Owners (IAOs):*** these are the people who compile specific information and their role is to be clear about:

   a) what information they hold, and for what purposes
   b) how this information will be amended or added to over time
   c) who has access to the data and why
   d) how information is retained and disposed off

3. ***Network Manager*** *(or whoever oversees the network, monitoring its performance, security, error detection, and implements access controls)* Some critical elements of e-Security procedures are the responsibility of Technical Support Staff (see particularly but not exclusively Access Control (the Network) no. 4 below, and Technical Security no.10 below). The roles of Technical Support Staff will differ in different phases of schools. As a general rule, ICT technician capacity should be on a similar level to school office capacity.

Although these roles are specifically referred to in the procedures below, the maintaining of data securely is everyone's responsibility - whether they are a member of staff, a student, a parent or a governor. Failure to apply agreed controls to secure data can be a serious matter, even resulting in legal action. For further information about roles and responsibilities, go to:

www.becta.org.uk/fits_om/security_administration/roles_responsibilities.cfm

Roles and Responsibilities. *Ask yourself...*

- ? *Does your school have a co-ordinated team approach to e-Safeguarding?*
- ? *Do you have a designated Senior Information Risk Officer (SIRO)?*
- ? *Have you designated Information Asset Owners for your organisations important information?*
- ? *Do you have a designated Network Manager?*

e-Safeguarding Procedures

1. **Risk Assessment** (Responsibility: Senior Leadership Team)

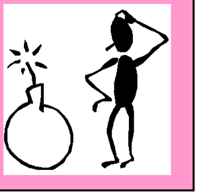
   e-Security and e-Safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of ICT is completely risk free. Information security is critical, in both protecting the information held concerning staff and pupils, and in ensuring the reliability of ICT systems to support teaching and learning.

   As a minimum, the risk assessment shall be updated and reviewed by the Senior Leadership Team annually and reported to the Governing Body. It is recommended that a review should be conducted each term.

   [For a suggested Risk Assessment Structure, see the Risk Assessment Form on Page 20]

Risk Assessment. *Ask yourself…*

- **?** *Do you have in place a Risk Assessment for data security?*
- **?** *Who does it?*
- **?** *How is it done?*
- **?** *How often is it done?*
- **?** *Who is it reported to?*
- **?** *Is follow up action monitored?*



2. **Information Classification** (Responsibility: All Staff)

   Following many recent breaches of information confidentiality, current government guidance for schools is to align school information with three government information classification levels. These classification levels are derived from the potential impact that unauthorised disclosure of information may have on the individuals concerned.(Please see glossary for full explanation of the following headings)

   i) **Restricted:** Information which can only be accessed by named individuals or groups. ***Printed restricted information shall be labelled to identify it as confidential.*** Where possible, restricted information on screen should be labelled as such.

   ii) **Protect:** General school information which it is not expected to be released to the public.

   iii) **Public:** Information freely available to anyone.

Schools should compile and annually update an information classification table on the lines of the one started below. This should be reported to the governing body. For requirements related to access, see Access Control below.

Restricted	Protect	Public
Personal information related to pupils or staff (usually contained in the Management Information System).	School routines, schedules and management information.	Website and promotional materials. Display material around school.

Information Classification. *Ask yourself…*

? *Who decides how school data is classified?*

? *How do users know the classifications?*

? *When is it updated?*

Access Control: Systems Access (Responsibility: Senior Leadership Team)

a) ***Access to all ICT systems shall be via unique login and password. Any exceptions shall be guidance in the risk assessment, and approved by the SIRO.***

b) 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 SIRO.***

c) ***All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the SIRO. This shall include the authorisation of access required by the ICT Support Team during investigations.***

d) ***Where 'restricted' information is stored, access shall only be granted to individuals approved by the SIRO. A record shall be kept of these approvals.***

e) All access controls should be reviewed each term, to ensure that any users that leave have their access removed.

4. **Access Control: The Network** (Responsibility: Technical Support Staff)

a) Where any external network traffic is allowed from the Internet to the school, a local firewall shall be deployed to restrict traffic to only necessary ports and IP addresses.

b) Where the school's external Internet connection allows connections from other schools behind a shared firewall, a local firewall should be considered to restrict this traffic.

c) 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.

d) Where externally facing services may be at particular risk, the addition of an Intrusion Prevention System (IPS) should be considered.

e) The use of external specialist third-party penetration testing should be considered on an annual basis for Internet visible systems.

f) 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.

g) The use of shared folders on workstations and laptops should be discouraged. If used ensure folders are password protected.

h) Note also section on Remote Access below.

Access Controls. *Ask yourself…*

? *Are user names and passwords in place?*

? *Are logins related to the information classifications?*

? *Is the Network secure?*

5. **Use of ICT Systems** (Responsibility: All Staff)

a) ***All users of ICT systems shall take responsibility for their own use of technologies,*** taking appropriate steps to ensure that they use technology safely, responsibly and legally. Inappropriate use exposes the school to risks including virus attacks, compromise of network systems and services, legal issues, and potentially even pupil safety.

b) Staff and pupils should be aware that all school ICT activity and on-line communications may be monitored, including any personal and private communications made via the school network.

c) Schools shall include appropriate training for all sectors of the school community. This should cover:

i) School Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.

ii) School 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.

iii) A comprehensive and developmental e-safety curriculum for pupils referenced in schemes of work and programmes of study. The programme should include the responsible use of web and communication technologies both inside and outside school and risks related to cyber-bullying.

iv) Regularly re-visiting of the AUP with staff and pupils.

v) ICT non-teaching staff training related to how ICT can enhance learning and teaching (see Becta's FITS programme)

Organisations like ChildNet, ThinkUKnow, CEOP, Becta offer support for education and training materials.

d) Schools shall create a working Acceptable Use Policy (AUP) based on all the agreed procedures for e-Security and e-Safety and covering ICT usage by all sectors of the school community(See Becta **AUPs** in context) ***This policy shall be subject to annual review by the governing body.***

e) In the light of the creation of the AUP, schools should consider how all sections of the school community engage with it e.g. signed agreements accepting the AUP.

f) Schools should also engage all parents and carers in the safe and responsible use of ICT in general and the contents of the AUP in particular. The Learning Platform is a valuable means of engaging parents and schools should consider what they have on the Learning Platform for the use of parents.

Use of ICT Systems. *Ask yourself…*

- **?** *Is on-line activity monitored?*
- **?** *Is e-Safety education regularly re-visited by staff and students?*
- **?** *Does the AUP accurately outline how all procedures are carried out?*

6. **Password Security** (Responsibility: All Staff)

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

a) Keeping their password secure from pupils, family members, and other staff.

b) Using a different password for accessing school systems to that used for personal (non-school) purposes.

c) Choosing a password that is difficult to guess, or difficult for pupils to obtain by watching staff login.

d) Adding numbers or special characters (e.g. !@£$%^) can help.

e) Changing passwords regularly e.g. each school term.

f) Staff should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.

g) In addition, when leaving a computer for any length of time, all staff shall log off or lock the computer, using CTRL+ATL+DELETE.

f) Ensuring that there is a limit on the number of consecutive failed log in attempts. (Best practice is between 3 and 5 attempts)

g) Restrict concurrent access i.e. a user should not be able to log in at the same time from two different machines.

h) Access credentials (passwords) should not be stored within the machines internet browser or any remote access software.

Password Security. *Ask yourself...*

? *Is there a clear policy regarding password conventions and renewing?*

? *Is it monitored?*

7. **Incident Reporting** (Responsibility: Senior Leadership Team)

An important element of e-Safeguarding is the ability to identify and deal with incidents related to the confidentiality of information. All staff and pupils 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 on the school. ***The Senior Leadership Team shall establish an incident reporting procedure and record reported incidents in an Incident Log.*** This log should capture the following information:

Incident Date: When the occurrence took place	**Description of the Occurrence:** What happened inc. classification of any information compromised	**Immediate Corrective Action:** What was done to minimise the impact of the incident	**Further Action:** Tasks to be undertaken to prevent re-occurrence	**Legal Implications:** Any legal ramifications e.g. data protection act	**Closed Date:** Date by which the incident is closed by the Head/SIRO

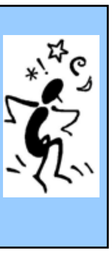
The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Senior Leadership Team at a minimum frequency of once per term. Through this review process, where deemed appropriate management shall update the risk assessment in light of new incidents. The Log and accompanying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

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

- Circumventing the network security system
- Accessing inappropriate material (definition should be in AUP)
- Installing unapproved software
- Using other people's 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

Incident Reporting. *Ask yourself...*

- **?** *Do you have an incident reporting mechanism?*
- **?** *Is everyone clear about how to report an incident?*
- **?** *Who holds and monitors the Incident Log?*
- **?** *Is action taken when an incident is reported?*



8. **Starters and Leavers** (Responsibility: Senior Leadership Team)

a) ***The Senior Leadership Team shall ensure that the ICT Technical Support Team are informed promptly of any member of staff joining or leaving the school.***

b) Any school owned ICT equipment should be returned to the ICT Support Team when staff leave.

c) The ICT Support Team shall ensure that leavers' access is removed, or disabled, in a timely manner. This communication should take the form of an email from the office to the ICT Support department.

d) The Senior Leadership Team shall have a similar process for pupils starting or leaving the school.

Starters and Leavers. *Ask yourself...*

- **?** *Do you have a starters and leavers procedure?*
- **?** *Who enters and removes staff and students from the system?*
- **?** *How does this person get the information?*

9. **Remote Access** (Responsibility: All Staff)

The use of mobile computing devices and connecting to the schools network from home is increasingly important but presents a number of security risks which need to be addressed. Users of mobile computing facilities (such as laptops) are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or damage of such items, and to prevent unauthorised access to information held on the device. Particular care should be taken when leaving devices in cars, hotel rooms, or the home, ensuring that they are not visible. Where possible, mobile devices should be locked away when not in use.

The following guidelines shall apply when accessing systems and information away from the school:

- ***a) Only necessary information should be stored on the device***

- ***b) Pupil sensitive (restricted) information shall not be stored on any mobile devices unless encrypted***

The removal of any ICT equipment, information and software from school premises shall only be permitted with prior authorisation from the ICT Co-ordinator, SIRO, or Head Teacher.

Educational organisations should use secure remote access technology, where appropriate, to secure the personal data of learners, staff and any other authorised users. Organisations should base their remote access requirements on information Risk Assessments. Organisations should think carefully about what kinds of sensitive and personal data they are making available remotely and who they are granting access to.

In addition, there are some key technical requirements for remote access which need to be in place in all schools:

- ***a) All user remote access shall require a username and password.*** Where access is given to information classified as '**Restricted or Protect'**, access should have two-factor authentication.

- ***b) Where third-parties require remote access to support systems, this shall be allowed through VPN with SIRO approval.*** Where possible, third-party access should only be enabled when required.

- c) All remote access should be subject to account locking after a maximum of 5 failed attempts.

Remote Access. *Ask yourself…*

- **?** *Is the system set up to enable users to securely access the network from outside the organisation?*
- **?** *Are there rules about taking ICT equipment off the school premises?*
- **?** *Do you take any specific precautions to ensure the safety of the data held on mobile devices?*

10. **Technical Security** (Responsibility: Technical Support Staff)

a) ***All externally facing devices shall be hardened and patched to ensure no high-risk vulnerabilities are present.*** This should normally mean that all security updates are applied within one month of release by the vendor. All other internal systems should be regularly patched with the latest security updates, ideally prior to the commencement of each term.

b) The use of a scanner, to help identify high-risk vulnerabilities, should be considered.

c) All desktops shall have up-to-date anti-virus software installed.

d) All incoming email shall be scanned for viruses, and should be filtered for spam.

e) All virus definitions shall be updated daily.

f) All anti-virus shall be configured to alert the ICT support team when any virus is detected.

g) Where possible, the use of memory sticks and other mobile storage media should be restricted, or scanned for viruses each time they are connected.

h) All pupil access to the Internet shall be filtered for inappropriate content.

i) All hard disks, and other media containing school information shall be securely deleted, either by specialist deletion utilities or physical destruction, prior to disposal.

j) Data backups should be automated, taken at regular intervals (daily) and backup media should be kept offsite. Backup media should be subject to the same security controls, and destruction procedures as other ICT storage devices.

k) Consideration should be given to procedures for security logging. The following are suggested as a starting point.

i) A log consolidation tool should be considered to help with the analysis of logs. Such tools can also help with the secure archiving of logs.

ii) In order to ensure that logs across multiple devices correlate, the time of each ICT device should be synchronised by using a network time protocol server.

Target logs	***Reason(s) for logging***	***Recommended review frequency***
Internet access	Facilitate investigations and pupil disciplinary procedures	Weekly random sample checks to support pupil monitoring
Detected viruses	Remove malicious software, and to identify infection route	Following automated alert
Failed login attempts	Identify attempted unauthorised access	Weekly review
Emails sent and received	Facilitate investigations and pupil disciplinary procedures	As required to support investigations
Blocked firewall traffic	Assist with identification of malicious activity, and mis-configurations	Monthly review
Windows servers security events	To help with general troubleshooting and investigations	As required to support investigations

Technical Security. *Ask yourself…*

- ? *Do all computers in your school have Anti-Virus software installed?*
- ? *Are your Technical Support Staff automatically alerted if a computer detects a virus?*
- ? *Do you regularly update your computer operating system?*
- ? *Do you filter all internet usage preferably with a Becta approved system?*
- ? *Do you perform data backups?*

Next Steps.

1. *Use the checksheet (Page 21) to assess your immediate and longer term priorities*
2. *Consider if there is potential for collaboration with other local schools to achieve your objectives*
3. *Create an action plan (page 22) and inter-relate the plan with the School Improvement Plan (The online tool can be used to support the creation of an action plan)*

Glossary of ICT Terms

API: Acronym for Application Program Interface, a set of tools, routines and rules for building software applications in a consistent way.
ASP: Specialist Internet service provider (ISP) that allows a corporate clients to have a software application (e.g. an e-Learning Platform) hosted in exchange for a rental fee.
Asynchronous Learning: Mode of learning event in which participants are not online at the same time and are unable to communicate without time delay.
Authentication: Process of confirming the identity of an individual.
AUP: Acronym for Acceptable Use Policy i.e. agreed procedures in place to minimize e-security and e-safety risks
AVI: Acronym for Audio Video Interleave - the file format used by Microsoft Video for Windows.
Bandwidth: Term that describes how much data can be sent via a connection in a specified time. This measurement is typically described in bps or bits per second.
Becta: British Educational Communications and Technology Agency: government funded agency promoting use of ICT
Bit: The minimum unit of computer data - either a 0 or a 1.
Blog: A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.
Bps: Acronym for Bits per second the units in which the speed of modems are rated. Indicates the amount of information a modem can transmit and receive each second.
Browse: Process of viewing web pages over the World Wide Web.
Browser: Program that allows you to view and interact with web pages on the World Wide Web.
BSF: Building Schools for the Future (government funded program)
Byte: Unit for measuring data - usually 8 bits.
CEOP: The Child Exploitation and Online Protection Centre delivers a multi-agency service dedicated to tackling the exploitation of children.
CD: Acronym for Compact Disc. Originally an audio-only format the CD has spawned a range of derivatives including CD-ROM (Compact Disc Read Only Memory), CDi (Compact Disc Interactive) CD-R (CD-ROM Recordable) and most recently CD-RW (Compact Disc Read Write).
Chat: Talking to one person or many people, usually in text format via the internet
Childnet: A non-profit organisation working with others to help make the Internet a positive and safe place for children.
Compression: Reducing the size of a file so that can be transmitted more quickly and takes up less storage space
Cookie: Small element of data sent to your computer when you a website. When you subsequently return to the site this data may be used for a range of things including recalling your username.
DHTML: Acronym for Dynamic HTML, a new way of developing web pages with enhanced functionality. Standards for DHTML are still being developed.
Digital: Made up of zeros and ones (or bits of information)

DNS: Acronym for Domain Name System the system that regulates naming of computers on the internet. The core of the system is a vast database that stores the names and network addresses of every computer, accessed whenever a computer needs to convert a Domain Name into a numeric IP address

Domain: Official name for a computer attached to the Internet. Email addresses normally consist of a user ID and a domain name separated by the @ symbol

Download: The process of copying files from one remote host to your computer, usually via FTP.

DVD: Acronym for Digital Versatile Disc

e-Learning: Wide range of electronic learning applications and processes including Web-based learning, computer-based learning, virtual classrooms and digital collaboration. Commonly held to include delivery of content via Internet, intranet/extranet (LAN/WAN), audio/video tape, satellite broadcast, interactive TV, and CD-ROM.

Email: Sending electronic messages over a network or the internet.

e-Security: procedures to ensure all electronic data is categorised as public, restricted or protected and that electronic systems containing the data are securely maintained

e-Safety: procedures to ensure computer users know their access rights and responsibilities in using ICT.

Extranet: A local area network (LAN) or wide area network (WAN) using TCP/IP, HTML, SMTP, only available to people inside and certain people outside an organization, as determined by the organization.

FAQ: Acronym for Frequently Asked Questions. Answers to FAQs are an essential component in any effective website.

Flash: A vector graphic animation tool marketed by Macromedia and widely used for developing web delivered e-learning.

FTP: Acronym for File Transfer Protocol. Process that allows you to transfer files or programmes to or from computers across the internet.

GIF: Acronym for Graphics Interchange Format, a common format for the storage of largely non-photographic imagery.

Gigabyte: 1024 megabytes of computer data

Hardware: Physical technology such as computers, monitors and keyboards rather than software.

Hits: The number of requests for information made to a server.

Host: Computer that exists to allow other computers to connect with it.

HTML: Acronym for Hypertext Mark-up Language -the basic language that is used to construct web pages. There are several HTML standards in existence, the latest of which is HTML 4.

HTTP: Acronym for Hypertext Transfer Protocol, the standard that regulates the way information is transferred around the World Wide Web.

Hyperlink: Underlined word or set of words that, when clicked, takes you to a different place on that page or to a new destination altogether.

IAO: Acronym for Information Asset Owners; people who compile and have responsibility for specific online information

ICT: Acronym for Information and Communication Technologies

Internet: The full range of networks interconnected via TCP/IP protocol.

IP: Acronym for Internet Protocol, the rules that regulate the way information is transferred across the Internet.

IPS: Acronym for Intrusion Prevention System; a network security device that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities.

ISP: Acronym for Internet Service Provider, companies that provide users with access to the internet.

Intranet: A private network inside an organisation that uses Internet technology, but is segregated from the Internet by a firewall. This means that authorised users can only access this network.

ISDN: Acronym for Integrated Services Digital Network. This telecommunications technology provides increased bandwidth using telephone lines but generates significant additional cost.

Java: Language developed specifically for creating software that can be simply downloaded from the Internet, but now used for a wide range of applications.

Javascript: Language similar to Java but actually incorporated into web pages in the interests of creating various special effects.

JPEG: Acronym for Joint Photographic Experts Group, the committee that originally developed this special image file format. JPEG files are now the most popular format for storing photographic images on the World Wide Web.

Kilobyte: Unit of computer data, made up of 1024 bytes.

LAN: Local area network, internal to your establishment.

Learning Platform: A Virtual Learning Environment with facilities for communication, work storage and access to learning resources

Learning Portal: Web site that offers learners consolidated access to learning and training resources from multiple sources.

Login: The acts involved in entering a computer system or the account name you have been allocated to gain access.

Megabyte: Unit of computer data made up of 1024 kilobytes.

MIS: Acronym for Management Information System; provides a co-ordinated approach to the gathering and use of data

Modem: Device that allows one computer to connect to another via a telephone line.

MPEG: Acronym for Moving Picture Experts Group, the committee who devised this innovative file format for storing video images.

Network: Two or more computers connected together.

Network Manager: Someone who oversees the network, monitoring its performance, security, error detection, and who implements access controls.

Offline: Term that implies that an item of hardware or software is no longer actively linked with the Internet. See Online.

Online: Opposite of Offline i.e. an item of hardware or software is actively linked with the Internet.

Operating System: The basic system that underpins computer operations and the foundation upon which all other programs operate. MSDOS, Unix and Windows are all examples of operating systems.

Plug-in: Small pieces of software that add to the capability of existing programs.

PDA: An acronym for personal digital assistant which is a mobile device or palmtop computer.

POP: Acronym for Post Office Protocol or Point of Presence; the location where connections to a network or the Internet may be accessed via dial-up networking

Protect: General school information which it is not expected to be released to the public.

Public: Information freely available to anyone.

Remote Access: Accessing and/or processing data from a computer in a different location.

Restrict: Information which can only be accessed by named individuals or groups.

Router: Mechanism for transferring data between one or more networks.

SCORM: Acronym for the Shareable Courseware Object Reference Model standard developed by ADLNet

Server: Both the software and hardware that is used to provide access to an internet resource.

SIRO: Acronym for Senior Information Risk Owner; a senior manager who is co-ordinates and takes responsibility for action related to e-security and e-safety.

SMTP: Acronym for Simple Mail Transport Protocol. The almost ubiquitous standard that governs how email is sent and received.

Software: The files, data and programs that allow a computer to function but have no physical dimensions. By way of contrast see Hardware.

Terabyte: Unit for a vast amount of computer data, consisting of 1024 gigabytes.

Twitter: This is a free social networking and micro-blogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as followers.

Unix: Operating system for mainframe computers originally designed in the 1960s but still widely used worldwide.

Upload: Send files to another computer, usually via FTP.

URL: Acronym for Universal Resource Locator otherwise known as the address of a website.

VoIP: Acronym for Voice over Internet Protocol, or using the internet to transmit voice conversations, a technique increasingly used within virtual classroom systems.

Virus: Self-replicating software that propagates itself from one computer system to another, normally devised with malicious or mischievous motives.

VLE: Acronym for Virtual Learning Environment (See Learning Platform)

VPN: Acronym for Virtual Private Network which is a software application to create a private computer link between computers in different locations.

Web space: Amount of data capacity available for the construction of web pages, normally measured in megabytes.

Website: Collection of linked web pages with a common theme, created for the same purpose.

World Wide Web: A global information resource made up of interconnected web pages.

e-Safeguarding Risk Assessment Form

High Impact: Public exposure of restricted information leading to embarrassment, system downtime, or data corruption impacting learning & teaching.

Medium Impact: Exposure of protected information to a non-authorised third party, leading to outcomes listed above.

Low Impact: Internal exposure of information beyond authorised individuals leading to outcomes listed above.

e-Security and/or e-Safety issue (risk assess these plus others identified)	**Threat** (What could happen)	**Impact** [See definitions above] High: Score 3 Medium: Score 2 Low: Score 1		**Vulnerability** (What is it you do – or not do – that could lead to the threat materialising)	**Likelihood** High(3): next 6 month Medium(2): next 2 yrs Low(1): unlikely in next 2 years		**Total Score** (Impact x Likelihood; out of 9)	**Action Plan** (Either risk accepted OR actions to be taken to reduce risk)
Information (restricted/protected) taken out of school on laptop, email etc								
Use of mobile data storage e.g. memory sticks								
Use of Internet for data transfer and communication								
Pupil gaining access to restricted or protected information								
Remote access via school equipment or home computers								
Back up (storage)								
Password misuse or poorly managed								
Viruses and malicious software installs								
Inadequate staff and pupil training in e-security and e-safety								

E-Safeguarding Procedures: Position at ……………………………………………. (date)

Procedure	In Place	Partially in place	Not in place	Don’t know	Actions for consideration
Roles and Responsibilities: SIRO appointed, IAOs identified and listed, technician responsibilities specified					
1. Risk Assessment: Procedures established, assessments and remedial action plans documented					
2. Information Classification: Table created and system for classification labelling established					
3. Access Controls: *Systems access records* (who has access to what) and *Network security measures* established and implemented					
4. Use of ICT Systems: AUP ‘owned’ by everyone. On-going education & training programme for everyone					
5. Password Security: Minimum requirements in place					
6. Incident Reporting: Procedure in use and monitored with action taken as necessary					
7. Starters and Leavers: Procedures established and active for both staff and pupil records					
8. Remote Access: Minimum requirements in place					
9. Technical Security: Minimum requirements in place					
10.					

e-Safeguarding Action Plan Template

What will be done	*Resource Implications*	*Target Date(s)*	*Indicator of Success*	*Person Responsible*