E-Safeguarding and Acceptable Use Policy

Contents

Introduction

We at Beecroft Academy recognise the importance of E-Safety and E-Security, this policy will outline the procedures we use to ensure all pupils and adults stay safe online.

Aims of the Policy

- To ensure everyone is aware of the procedures
- To be a working document which is reviewed yearly
- To clearly identify the roles of all adults and pupils involved at Beecroft Academy
- To raise children's awareness of E-Safety and what they can do to keep safe
- To outline teaching strategies, timescale and resources for staff to ensure effective coverage across the school
- To ensure Government policies and legal guidelines are being followed
- To make staff and adults aware of E-safety and how to identify, report and deal with an E-Safety concern/incident

Reviewing and Evaluating

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-Safety Champion (Mrs Willsher/Miss Williams)
- Headteacher (Mr A Haywood)
- Wellbeing Liaison Officer (Miss R Clark)
- Technician (Naveed – Comtech)
- E-Safety Governor
- School Council member

Roles and Responsibilities

School Management and e-safety

- School senior management is responsible for determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors of internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.
- e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and internet developments, current government guidance and school related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.
- e-safety provision is always designed to encourage positive behaviours and practical real world strategies for all members of the school and wider school community.

- Management is encouraged to be aspirational and innovative in developing strategies for e-safety provision which will deliver measurable success via a calendar of e-safety provision and clearly state e-safety targets with success criteria on the school development plan.

Evidence base:
- School development plan
- E-safety Action Plan
- Computing Long Term Plan
- Minutes from e-safety related meetings with staff, SLT, parents association, governors and wider school community stakeholders
- Regularly updated e-safety policy, child protection policy and logged and evaluated e-safety incidents.
- Staff inset provision audit and record.

The school e-safety Officer or Coordinator:
- The school has a designated e-safety officer [Mrs Willsher] who reports to the SLT and Governors and coordinates e-safety provision across the school and wider school community. The committee liaises with SLT, the schools designated Child Protection officer and other senior managers as required.
- The school e-safety coordinator is responsible for e-safety issues on a day to day basis.
- The school e-safety coordinator maintains a log of submitted e-safety reports and incidents.
- The school e-safety coordinator audits and assesses inset requirements for staff, support staff and governor e-safety training, and ensures that all staff are aware of their responsibilities and the school's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the school e-safety policy and safer internet practice, the e-safety Coordinator, the Child Protection Officer and ICT support are responsible for monitoring internet usage by pupils and staff, and on school machines, such as laptops, used off-site.
- The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.

Governors' responsibility for e-safety:
- At least one Governor is responsible for e-safety, and the school e-safety Officer/Coordinator will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.
- To provide and evidence a link between the school; governors and parents.
- An audit of Governor IT competence, relevant outside experience and qualifications is advisable to identify training needs and create a schedule and development plan. It is essential that Governors tasked with overseeing and monitoring e-safety have demonstrable experience, skills or qualifications to match the role.

ICT support staff and external contractors:
- External ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware.

- External contractors, such as VLE providers, website designers/hosts/maintenance contractors should be made fully aware of and agree to the school's e-safety Policy. Where contractors have access to sensitive school information and material covered by the Data Protection Act, for example on a VLE, school website or email provision, the contractor should also be CRB checked. It is best practice to keep long term maintenance and running of school VLEs, websites and email in-house, and only to outsource setup if required.

Teaching and teaching support staff:

- Teaching and teaching support staff need to ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.
- Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to internet and computer use in school.
- All staff need to follow the school's social media policy, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
- All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Child Protection Officer:

- The Child Protection Officer needs to be trained in specific e-safety issues. Accredited training with reference to child protection issues online is advised – for example a CEOP accredited course or a Cyber mentor course.
- The Child Protection Officer needs to be able to differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
- Possible scenarios might include:
    - Allegations against members of staff.
    - Computer crime – for example hacking of school systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

Pupils:

- Are required to use school internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
- Pupils need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.

- Pupils need to be aware that school Acceptable Use Policies cover all computer, internet and gadget usage in school, including the use of personal items such as phones.
- Pupils need to be aware that their internet use out of school on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities.

Parents and Guardians:

- It is hoped that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home.
- The school expects parents and guardians to sign the school's Acceptable Use Polices, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.
- The school will provide opportunities to educate parents with regard to e-safety.

Other users:

- Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.
- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be CRB checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

E-Safety and the Law

Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)

Copyright infringement and DMCA:

If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto site such as Facebook and Twitter.

Duty of care and 'in loco parentis':

Schools have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to school pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all schools, but especially to boarding and residential schools.

E-Safety Curriculum

E-Safety is incorporated into the schools Computing Curriculum (with strong links to Sex and Relationships Education as a part of PHSE). Lessons are planned using resources and materials from the 'Think U Know' website. The Computing and E-Safety Co-ordinator has taken part in CEOP Ambassador Training and can train up staff to use the resources so that they are able to train pupils in the school.

See the Computing Long Term Plan for more details on how E-Safety is covered in each year group.

How to deal with an E-Safety Incident

The precise chain of events for reporting an e-safety incident will vary depending on the Incident. Below are some examples, based on the nature and severity of the incident.

If you find illegal material on your network, or log evidence to suggest that illegal material has been accessed

- If the illegal material image is (or is suspected to be) a:
    - Child sexual abuse images hosted anywhere in the world
    - A non-photographic child sexual abuse images hosted in the UK
    - Or a criminally obscene adult content hosted in the UK
- Report to the CEOP - http://ceop.police.uk/safety-centre/. Contact your local police. Follow the school's child protection procedures if a child protection incident is suspected but: do not copy, archive, forward, send or print out the image – leave it in situ, and if in doubt seek advice from CEOP or your local police.

If there is a child protection issue:

If there is a child protection issue, the school policy will apply.

If there is illegal material which you are unable to remove which involves Grooming, or suspected child abuse via the internet:

Call your local police. Also contact CEOP http://www.ceop.police.uk/safety-centre/.

How to deal with e-safety incidents – indicative sanctions for pupils and staff:

Here are a list of Incidents which could occur

- Bypassing the school's filtering system:
- Viewing pornographic material:
- Illegal activities:
- Going on the internet in lessons or using websites not relevant to the lesson in lesson time:
- Using a mobile phone or other digital device in a lesson:
- Using social media (Twitter and Facebook) or email in lesson time:
- Cyber bullying:
- Writing malicious comments about the school or bringing the school name into disrepute – whether in school time or not:
- Sharing usernames and passwords:
- Deleting someone else's work or unauthorised deletion of school files:
- Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud using the school network:
- Uploading or downloading files using the school network:
- Copyright infringement of text, software or media:

Depending on the incident these procedures should be followed:

- Pupil: The class teacher will deal with the matter and write up an incident report to submit to the e-safety Coordinator. Staff: the issue may be raised by SLT to the Headteacher as a disciplinary matter.
- The Headteacher or delegated SLT with responsibility for pupil behavior (Miss Loudon) will deal with the matter.
- The person will receive a Reminder (depending on the severity of the incident) – See Behaviour Policy.
- The Police and IWF/CEOP should be contacted. Child Protection procedures take precedence over AUPs if CP is a factor.
- The External IT contractor should be contacted to obtain further evidence. (Comtech – Naveed)
- Depending on the severity of the incidence, the http://content.met.police.uk/Site/pceu cybercrime unit, http://www.actionfraud.police.uk/ or local police could be contacted.
- The Police and IWF should be contacted if indecent material was uploaded or downloaded. CEOP should be contacted if grooming / sexting or unwanted sexual advances were involved.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.

E-Safeguarding Procedures

E-Safeguarding Risk Assessment

The staff and governors at Beecroft Academy understand that e-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks. It is also understood that 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. Therefore, the senior leadership team are responsible for developing a risk assessment that will be updated and reviewed at least annually. It will also be shared with, and agreed by, the Health and Safety Committee of the governing body.

E-Safeguarding Action Plan

The risk assessment will be used to identify actions that need to be taken to improve e-safeguarding procedures at the school and the centre. These actions will form the basis of the E-Safeguarding Action Plan.

E-Safeguarding Procedures Review

E-safeguarding procedures will be reviewed at least termly by the Governors' Health and Safety Sub-Committee. The review will include consideration of both the risk assessment and related action plan.

Information Classification

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.

Restricted: information which can only be accessed by named individuals or groups. Printed restricted information should be labelled to identify it as confidential and stored in locked cupboards. Where possible, restricted information on screen should be labelled as such.

Protected: general school information which it is not expected to be released to the public.

Public: Information freely available to anyone.

E- Information Classification Table for Beecroft Academy

Restricted (Named Staff Only; Named Parents Only; relevant personnel in LA; Governors for Relevant Information.)	**Protected (All in School Community; relevant personnel in LA)**	**Public (Anyone)**
Personal information related to pupils or staff (usually contained in the Management Information System) – any information that identifies an individual.	School routines, schedules and management information.	Website and promotional materials. Display material around school.
• Integris • Individual pupil records e.g. 'Common Assessment Frameworks' forms, special educational needs paperwork, safeguarding paperwork, referrals, one-to-one tutoring paperwork • Information related to support groups e.g. booster programmes, nurture groups • Assessment information, including pupil tracking information (E-Profile, ASPIRE, Tapestry) • Annual reporting system • Class information • Dinner registers • Single Central Record • Finance packages	• Learning platform • Evolve – trips and visits information	• School website

NB The staff and governors at Beecroft Academy understand that this area of e-safeguarding is everyone's responsibility in order that children are kept safe.

Access Control: Systems Access

At Beecroft Academy we understand the need to carefully manage access to our electronic systems. In order to be e-secure we will ensure that:

- Access to our ICT systems will be via unique login and password and that any exceptions shall be documented in the school's E-Safeguarding Risk Assessment, and approved by the Headteacher.
- All information storage, where possible, shall be restricted to only necessary users and that limited access be granted to new groups of users (for example, an external group attending a school-based event) by the use of guest passwords. This access shall be approved by the E-Safety Lead.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil

personal storage) will be authorised by the E-Safety Lead. This shall include the authorisation of access required by the ICT Support Team during investigations.

- Where 'restricted' information is stored, access will only be granted to individuals approved by the E-Safety Lead and a record shall be kept of these approvals.
- All access controls will be reviewed each term, by the ICT technician, to ensure that any users that leave have their access removed.

The senior leadership team takes overall responsibility for ensuring these access control procedures are in place.

Access Control: The Network

At Beecroft Academy and the Beehive Children's Centre we understand the need to carefully manage access to the organisation's network. In order to be e-secure with regards to the school's network we will ensure that:

- We buy into the Central Bedfordshire Broadband Package which currently provides full filtering, antivirus and firewall protection for pupil and staff access to the internet. Any alternative provider will have to have the same protection or better.
- The antivirus suite on every computer is updated on a regular basis, whenever updates are issues by the AV provided.
- Laptops used outside the school and connected to any local area network (LAN) or wider area network (WAN or internet) must have an up to date independent firewall in addition to the antivirus programme.
- Users of laptops on a home connection must be made aware that they are not protected by the undesirable site filtering and firewall offered as part of the Central Bedfordshire Broadband Package.
- All USN memory sticks containing pupil details or management information must by encrypted.
- Management computer systems must be secured by adequate password and file sharing restrictions.

The ICT Technician takes overall responsibility for ensuring these access control procedures are in place.

Use of ICT Systems

At Beecroft Academy we understand the need to carefully manage access to the organisation's network. We will ensure that:

- All users of our ICT systems will take responsibility for their own use of technologies, taking appropriate steps to ensure that they use technology safely, responsibly and legally; it is understood that inappropriate use exposes the school to risks, including virus attacks, compromise of network systems and services, legal issues, and potentially even pupil safety.
- The staff and children are aware that all school ICT activity and on-line communications may be monitored, including any personal and private communications made via the school network. (N.B. In order to facilitate this staff will need to let the ICT technician know their password and then change their password).
- Related training is provided, as deemed appropriate, for all sectors of the school community; the training will help staff to:
  - Understand the rationale for all e-safeguarding procedures and the consequences of inappropriate practice
  - Take 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.

- Provide a comprehensive and developmental e-safety curriculum for children (both in school and in the Children's Centre) referenced in schemes of work and programmes of study (the programme will include the responsible use of web and communication technologies, both inside and outside school, and risks related to cyber-bullying).
- Regularly re-visit the school's e-safeguarding policies

NB Sources of support for education and training is on the school's Learning Platform (It's Learning) and can also be gathered from materials produced by organisations like ChildNet, ThinkUKnow, CEOP, Becta.

- Parents/carers will also be encouraged to engage in the safe and responsible use of ICT; Parents and Carers are invited into school to take part in workshops and training throughout the year and are provided with information through the school website and through leaflets and flyers. Also, the extended service will work with the school to provide related guidelines, support and advice for parents/carers.

Password Security

It is fully understood by all staff at Beecroft Academy that we are responsible for 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 with access to ICT systems will be responsible for taking the appropriate steps to select and secure their passwords. These steps will include:

- Keeping passwords secure from pupils, family members, and other staff.
- Using a different password for accessing school systems to that used for personal (non-school) purposes.
- Choosing a password that is difficult to guess, or difficult for pupils to obtain by watching staff login, and changing passwords regularly - each school term (NB adding numbers or special characters, or a phrase can help).
- Staff will try not write down their passwords, 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 will log off or lock the computer (using CTRL+ATL+DELETE).
- Guest passwords will be used on school laptops so that supply teachers, children etc can only access information relevant to them.

Technical Security

It is fully understood by all staff at Beecroft Academy that we are responsible for technical security. Technical security will be achieved by ensuring that:

- All externally facing devices are hardened and patched to ensure no high-risk vulnerabilities are present (NB this should normally mean that all security updates are applied within one month of release by the vendor and all other internal systems are regularly patched with the latest security updates, ideally prior to the commencement of each term).
- The use of a scanner, to help identify high-risk vulnerabilities, will be considered.
- All desktops will have up-to-date anti-virus software installed.
- All incoming email will be scanned for viruses, and will be filtered for spam.
- All virus definitions will be updated when necessary..
- All anti-virus will be configured to alert the ICT Technician when any virus is detected.
- Where possible, the use of memory sticks and other mobile storage media will be restricted, or scanned for viruses each time they are connected.

- All pupil access to the internet will be filtered for inappropriate content.
- All hard disks, and other media containing school information, will be securely deleted, either by specialist deletion utilities or physical destruction, prior to disposal.
- Backup media will be subject to the same security controls and destruction procedures as other ICT storage devices.
- Consideration will be given to procedures for security logging (NB the following are suggested as a started point).
- A log consolidation tool will be considered to help with the analysis of logs (NB such tools can also help with the secure archiving of logs).
- Logs across multiple devices correlate, the time of each ICT device will be synchronised.

Target logs	***Reason(s) for logging***	***Recommended review frequency***
Internet access	Facilitate investigations and pupil disciplinary procedures	Regular random sample checks to support pupil and staff 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

Beecroft Academy

E-Safeguarding Incident Report Record

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

Parent and Pupil Acceptable Use Policy

Staff Acceptable Use Policy

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