Great Baddow High School

eSafety
and
Data Security

GBHS Adaptation v1 – May 2015

For review annually

Reviewed and adopted by the Governing Body: June 2016

CONTENTS

Introduction

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

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

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

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

At **Great Baddow High school** we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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

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

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

Monitoring

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school and its internet provider. These logs may be monitored by authorised staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the head teacher as the school's Senior Information Risk Owner (SIRO), directly or via the network manager or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SIRO.

See flowcharts on pages 29 & 30 for dealing with both illegal and non-illegal incidents

An example security breach report can be found on the Essex Schools Infolink>Information Governance>Security Breaches.

Great Baddow High School

Acceptable Use Agreement: Students

This Acceptable Use Policy has been written to ensure every one of our students understands our expectations and knows the rules for using the computer resources. We look for your support and hope you can find the time to discuss the main issues mentioned below before signing and returning this form to the school.

Using our Internet and E-mail facilities

The School provides every student with a fast filtered broadband connection to the Internet, but this does not guarantee students will not find a way to view unsuitable material.
The School also encourages everyone to develop their communication skills by using electronic mail.
We acknowledge the privacy and rights of every student and will investigate where our filtering system shows inappropriate or offensive language or attachments have been included.
Your child needs to understand the seriousness of actions listed above when using the Internet and Email.

Acceptable use of the Equipment

Students will respect all our computer equipment to ensure our network continues to work reliably.

The Rules of Acceptable Use

Failure to observe these rules will result in appropriate disciplinary action. Depending on the severity of the act, this may include restricted access to ICT facilities, detention or exclusion.

Your son or daughter needs to agree to the following rules:

- Only log on using their own unique username and password and keeping these secret;
- Students should not bring or download unauthorised programs, including games. Online non-educational internet games are not an appropriate use of school resources;
- The personal use of chat rooms and instant messaging is banned, though they may be experienced within the ICT curriculum;
- Ensure text, emails, images, sounds or video's they may view or send do not offend or upset any person, or damage their reputation, or that of the school;
- Students must not distribute or import from data stick, disk or other portable storage device materials to others which could be classed as offensive, obscene, bullying or damaging;
- Students must not scan, digitally photograph or modify any images that could be classed as offensive, obscene, or damaging;
- Students must ensure all their own work is original, they must not copy or do work for another. Plagiarism (copying someone else's work) is a serious issue, it is cheating and exam boards will ban students;
- Students must not store the following types of files in their home directory, without permission from the Network Managers or a computing teacher: Program files (EXE, COM) Compressed files (ARJ, LHZ, ARJ, TAR etc) Music Files (MP3 MP4 WAV CDA);
- When using the internet students should not attempt to search for, access, attach, view, import, distribute or send any material which could be classed as offensive, obscene or damaging;
- Students should not reveal their personal address or phone numbers or those of students or staff.

  The full copy of the eSafety and Data Security policy will be available from the School Reception or via our website www.gbhs.co.uk

Consent for school use of photography for special purposes

In order to comply with the Data Protection Act 1998 respect of personal data and in line with LEA guidelines, we need to ask for your consent to being photographed (including digital and video images) where we propose to use the images for publicity purposes. This includes posting them on a website, in a school brochure or in parts of the school to which the public has access.

We may also include images in the school brochure, DVD and website, and would like to use a variety of pictures and video images, some of which may include yourself. We will not, however, include the full names of any

students with their image. The school brochure and website are very important elements in promoting Great Baddow High School in the wider community and celebrating the achievements of our students.

We also use images of students on the interactive information display boards in the dining hall and in reception. This promotes your work to other students and visitors to the school.

Images of students cannot be used unless consent has been given. We would therefore be grateful if you could return the reply slip to give consent to being included in any such pictures and images. The pictures and images will not be used for any other purpose than stated above.

Student Statement

As a school user of the Network & Internet I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Signature	Date

Parent/Guardian Statement

As the parent or legal guardian of the student signing above, I grant permission for my son/ daughter to use the school network, electronic mail and the Internet. in the manner described above I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter/son to follow when selecting, storing and exploring information and media. I understand a breach of the stated protocol can result in school sanctions being applied.

Student Name	Tutor Group
Parent Signature	Date

Photography Consent Form

Student Name	Tutor Group

I give my consent to appearing in photographs and video images taken for inclusion in the school's brochure, DVD and website.

I do not wish to appear in photographs or video images of activities for inclusion in the school's brochure, DVD or website.

Signed	Date

Great Baddow High School

Acceptable Use Agreement: Staff, Governors and Visitors

Policy for: **The Acceptable Use of Computers, The Network and Data systems**

This Acceptable Network Use Policy has been written to ensure every member of staff understands our expectations and knows the requirements for using the computer resources and network system. Where appropriate, parts of this policy document will be used to inform the student network use policy.

INTERNET AND E-MAIL FACILITIES

The School provides every member of staff and student with a fast filtered broadband connection to the Internet, but this does not guarantee unsuitable material cannot be accessed.

Everyone is allocated an e-mail account and the School encourages everyone to develop their communication skills by using electronic mail.

We acknowledge the privacy and rights of every member of the school community but will not allow the school system to be the vehicle of bullying or intimidation and will investigate where our filtering system shows inappropriate or offensive language or attachments have been included. All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network or with school equipment. In addition all internet activity is logged by the school's internet service provider. These logs may be monitored by authorized Academy and county staff.

ACCEPTABLE USE OF EQUIPMENT

1. Staff have a duty to take care of all our computer equipment to ensure our network continues to work reliably. Security of the school equipment and system is paramount. Laptop computers are the personal responsibility of the member of staff they were issued to and must be kept either with the member of staff or locked into place at all times. A Kensington cable is available from the network manager's office to secure laptops to the teacher desk. If a lockable cupboard or filing cabinet is not available in the classroom or the department one can be provided for you.
2. The allocated keeper of a school laptop is entirely responsible for the documents and websites viewed on it both in and out of school, including third party use which is to be discouraged.
3. Staff should be aware of the Health & Safety guidance regarding the school system and follow this at all times[1]

ACCEPTABLE USE OF DATA

1. The school has a legal responsibility to ensure that all personal data, for the whole school community, is kept in accordance with The Data Protection Act (1998) and as such holds members of staff responsible for any transfer and storage of personal data.
2. Wherever possible data should be kept only on the school network and administration systems. Where it is essential that documents and data are stored on a portable laptop or other portable storage devise it is imperative that this data is encrypted, encoded or otherwise protected and secure. Reports and student assessment data may be kept on a laptop computer in the short term but may not be permanently stored on a portable storage devise (such as USB stick). Any letters written in the pursuance of your duties must be stored without any identifying names or addresses, any student details held on a portable device or laptop must be vague enough to ensure that the child cannot be identified by a third party.
3. When leaving a laptop or computer staff must ensure that they are logged out or that the keyboard is locked to ensure data and system security.

RESPONSIBILITIES

1. You should use our computer facilities with care, respect and in a safe manner respecting other users.
2. Only log on using authorised usernames and passwords and keeping these safe;
3. You should not upload or download unauthorised or unlicensed programs, any software you wish to be added to the school system must go through the network managers, who should where possible be involved in its purchase to ensure system compatibility.
4. Ensure text, emails, images, sounds or video's you may view, post or send are not libellous, obscene, defamatory, seditious, blasphemous, do not seek to incite racial hatred or otherwise break the laws of

[1] See Health & Safety Policy or Health & Safety Officer for copies if required

the United Kingdom and do not offend any person, or damage their reputation, or that of the school;

5. You must not import from disk or distribute materials to others which could be classed as offensive, obscene, bullying, damaging or otherwise unprofessional; nor scan, digitally photograph or modify any images that could be classed as offensive, obscene, or damaging;
6. When using the internet you should not attempt to search for, access, attach, view, import, distribute or send any material which could be classed as offensive, obscene or damaging;
7. Staff should not reveal the personal data of students or staff to unauthorised persons nor permit access to this data by a third person, nor should personal data be revealed on any social networking site or blog;
8. Staff should be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies and encourage e-safety in our students.
9. Staff have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

Social networking between staff and students is discouraged both by the school and Essex County Council. Please be aware that this policy holds both whilst in school and out of school.

Failure to observe these rules may result in appropriate disciplinary action and could have legal implications.

I have read and understood the Policy for

The Acceptable Use of Computers, The Network and Data systems.

I agree to adhere to the policy details.

Full Name	
Job Role	
Signature	
Date	

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Great Baddow High School

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows Department for Education guidelines
http://www.education.gov.uk/schools/studentsupport/pastoralcare/b00198456/principles-of-e-safety and the Local Authority guidance documents listed below

The safe use of new technologies - Ofsted
http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies

Teachers and Governors Guidance
http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/HR/Workload_Agreement/Guidance_Docs/dfes-InformationManagementSkillsforSuccess.pdf

Internet filtering for Essex Schools
http://secure.essexcc.gov.uk/vip8/si/esi/dis/content/index.jsp?sectionOid=895&channelOid=24818&guideOid=79839&guideContentOid=79867

e-Safety Audit Tool - Information for Governors, Management and Teachers
http://www.nen.gov.uk/hot_topic

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff are aware of the relevant guidance documents available on the EGfL website
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

Safe Haven Fax procedures

When sending personally identifiable information:

- ensure the recipient knows the fax is being sent.

- ensure the fax will be collected at the other end.
- send the front sheet through first.
- check that it has been received by the correct recipient.
- add the rest of the document to the fax.
- press the **redial** button.
- don't walk away while transmitting.
- wait for the original to process and remove it from the fax machine.
- wait for confirmation of successful transmission.
- confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
- use only the minimum information and anonymise where possible

---

Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as private, although some data e.g. Child Protection data, should be restricted to CONFIDENTIAL.
- The caveat classifications that GBHS use are;
    - PERSONAL e.g. personal information about an individual being sent outside of the school network
    - PRIVATE e.g. for sensitive information about an individual or incident
    - CONFIDENTIAL e.g. sensitive personal information about an individual, often involving safeguarding or legal considerations
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- Very careful consideration should be given before printing any labelled documents or emails

---

Senior Information Risk Owner (SIRO)

The SIRO at Great Baddow High School is Carrie Lynch – Headteacher - and has the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. The school has identified the SLT, the network manager, the eSafety coordinator, Heads of Year and the business manager as Information Asset Owners.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, student or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAOs are able to manage and address risks to the information and make sure that information handling complies with legal requirements. Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

FIXED ASSET REGISTER, INVENTORY & DISPOSAL OF ASSETS POLICY

Fixed Asset Register

1. This is used for accounting purposes only and provides a basis for capitalisation and depreciation for assets with a value of £2,000 or over (exclusive of V.A.T.) – at the time of purchase – either individually or as a set.

   The register is maintained by the finance department and should include all items that make up the balances shown on the academy balance sheet.

Inventory

2. Governors recognise the need to maintain an inventory of equipment in the school in order to:-
   - ensure proper physical control of equipment;
   - provide a basis for insurance cover and claims if equipment is damaged or destroyed;
   - provide an up-to-date record of the equipment available for teaching purposes;

3. All items of equipment will be both visibly and invisibly marked with the name and postcode of the school. As and when they are received entries will be made in the inventory, in two sections, for:-
   - items valued at £1,000 (excluding V.A.T.) or more at the time of purchase, either individually or as a set;
   - items valued at £200 (excluding V.A.T.) or more and less than £1,000 at the time of purchase, either individually or as a set;

   The inventory should also include:
   - attractive and portable items;
   - items especially considered by the Headteacher as being worthy of inclusion.
   - Items hired to or leased by the school, that match any of the above criteria, will be included, but identified accordingly.

4. The inventory will be maintained by the Network Manager.

   For non-ICT equipment, it is the responsibility of the Head of Department to ensure that new items are added to the inventory by notifying them of equipment purchases. This will also enable the network team to security mark the items. A copy of the up to date list should be retained by the Head of Department.

5. The inventory for items over £1,000 will be checked at least once annually by the network management team, who should retain a signed printed copy of the list of items for filing and subsequent audit.

6. The departmental inventory will be checked at least once annually by Heads of Department, who should provide a signed printed copy of the list of items to the Network Manager for filing and subsequent audit.

   The Business Manager in liaison with the Network Manager will certify that these checks have been completed. All discrepancies are to be notified to the Headteacher immediately.

Disposal of Assets.

7. All disposals should be recorded promptly, showing the method of disposal and the authority for such action
8. The Governing Body has authority to dispose of surplus stocks, stores and assets with no upper limit as to their value. However, the Business Manager / Headteacher can dispose of surplus stocks, stores and assets to the value of £500 without prior authorisation from the Governing Body. All disposals to this value must be reported to the Finance & Premises Committee at the next possible meeting.

All disposals must be formally recorded in the minutes

9. Items which are to be disposed of by sale or destruction must be authorised for disposal by the Business Manager and, where significant, should be sold following competitive tender. The academy must seek the approval of the DfE in writing if it proposes to dispose of an asset for which capital grant in excess of £20,000 was paid.

10. The Finance & Premises Committee is responsible for authorising the disposal of individual items with an original purchase price of up to £5,000.

11. The Governing Body in conjunction with the Finance & Premises Committee is responsible for authorising the disposal of individual items with an original purchase price of between £5,001 and £20,000.

    The academy is expected to reinvest the proceeds from all asset sales (for which capital grant was paid) in other academy assets. If the sale proceeds are not reinvested then the academy must repay to the DfE a proportion of the sale proceeds.

12. Disposal of equipment to staff is not encouraged, as it may be difficult to evidence that the academy obtained value for money in any sale or scrapping of equipment. In addition, there are complications with the disposal of computer equipment, as the academy would need to ensure licences for software programmes have been legally transferred to a new owner.

13. All disposals of land or heritage assets must be agreed in advance with the E.F.A.

14. A separate 'Off Site Register' of Items removed from the school site shall be kept for all items loaned to members of staff and students and all items taken off site for any reason shall be entered.

    In the event of any items not being on site when the inventory is checked, reference shall be made to this register in the first instance. Laptops are in the permanent care of budget holders and it is therefore not required to sign the off-site register when these are removed from the School site.

15. A duplicate 'back up' copy of both inventories will be retained and stored securely and remotely (separate building) of the original - in case of emergency/ loss of the original register.

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, students must have experienced sending and receiving e-mails.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending e-mails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated account

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail

- Students are introduced to e-mail as part of the Computer Science Scheme of Work

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving school related e-mail is not permitted

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided wherever possible
- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s) – preferably by telephone
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

Great Baddow High School
- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

Future Developments

Essex county council are now using a web based email system sent whereby all sensitive communications are sent using GCSx. GCSx stands for the Government Connect Secure eXtranet. It provides a more secure communications system (i.e. more secure than the internet).

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a student, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top and bottom of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules.

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

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

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is *Cathy Kibble* who has been designated this role. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in the Computer science & ICT curriculum and in PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- Our staff receive information and training on eSafety issues in their initial induction and regular updates each September.
- Details of the ongoing staff training programme can be found with the Safeguarding team
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Social Media -The Appropriate and Professional use of Social Media

Great Baddow High School understands that social media and networking websites have become a regular part of everyday life and that many people enjoy membership of sites such as Facebook, MySpace or Twitter. However, we are also aware that these sites can become a negative forum for complaining or gossiping and care must be taken not to breach our confidentiality policy or offend anyone when using these services.

General Information

The following policy element has been designed to give staff clear guidelines as to what Great Baddow High School expect of them when accessing these sites. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of this policy. Where no policy or guidelines exist, employees should use their professional judgment and take the most prudent action possible. Consult with your line manager or a member of SLT if you are uncertain.

Guidance for Personal Use

If you have your own personal profile on a social media website, you should make sure that others cannot access any content, media or information from that profile that (a) you are not happy them to have access to; and (b) which would undermine your position as a professional, trusted and responsible person.
As a basic rule, treat it as public communication, if you are not happy for your colleagues, students or their parents to see particular comments, media or information simply do not post it in a public forum online. When using social media sites, staff members should consider the following:

- Changing the privacy settings on your profile so that only people you have accepted as friends can see your content.
- Reviewing who is on your 'friends list' on your personal profile. In most situations you should **not** accept friend requests on your personal profile from 'clients' you work with (This includes students, ex-students, parents, etc).
- Ensuring personal blogs have clear disclaimers that the views expressed are yours alone and do not represent the views of GBHS. Make your writing clear that you are speaking for yourself and not on behalf of GBHS.
- Ensuring information published on the Internet complies with GBHS confidentiality and data protection policies. Breach of confidentiality will result in disciplinary action and may result in termination of your contract.
- Ensuring you are always respectful towards:
    - Great Baddow High School
    - Other Staff Members
    - Parents and Families (including children and other relatives)
    - Other Agencies and Partners

Staff should be aware that any disrespectful comments to the above might be seen as libellous and could result in disciplinary action or termination of your contract.

- Great Baddow High School logos and trademarks may not be used without consent.
- At all times, in or out of working hours, you are an ambassador for the school. Be aware that your actions captured via images, posts or comments online can reflect on GBHS

Use of Official Accounts

Great Baddow High School operates a number of accounts on social media websites for the promotion of activities and events, and as a communication method. The following outlines the limits of their use.

- An official account on any social media website may only be set-up with written consent from the SLT.
- Only authorised staff may use these accounts to post online and access to the account should be strictly limited.

- All information published on the Internet must comply with GBHS confidentiality and data protection policies.
- Parents or children should not be referenced online without their express consent. This includes all photos, videos and other media.
- Copyright laws must be respected, with references or sources cited appropriately.
- Any employee who becomes aware of social networking activity that would be deemed distasteful should make their line manager aware as soon as possible.

All staff using official accounts must adhere to the above guidelines; breech of this policy may result in disciplinary action or termination of your contract.

Specific advice for teachers regarding privacy settings:

Facebook

http://en-gb.facebook.com/help/

Separate friends' lists and access settings

http://en-gb.facebook.com/help/?page=175076589213424

If evidence if needed to protect against false allegations download a record of all your Facebook interaction

http://en-gb.facebook.com/help/?page=116481065103985

Twitter

Remove private information

https://support.twitter.com/groups/33-report-a-violation/topics/166-safety-center/articles/18368-safety-private-information#

Report other violations and remove content

https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/15789-how-to-report-violations#

Deal with pictures copied without permission

https://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/15795-copyright-and-dmca-policy#

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the students at the start of each school year
- eSafety messages will be prominently displayed

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner. See Page 12.

eSafety Incident Log

The incident log includes a range of incidents some of which may need to be recorded in other places, if they relate to a bullying or racist incident. Details of ALL e-Safety incidents are recorded by the e-Safety Coordinator or pastoral team. This incident log is held as a secure document and is monitored termly by AHT Behaviour & Safety and annually by the Headteacher.

Student's Name (Perpetrator)	Nature of Incident	Others Involved	Action Taken	Outcomes	SEN FSM	CODE PV, VB, RC, FDS, THB, ES	Review

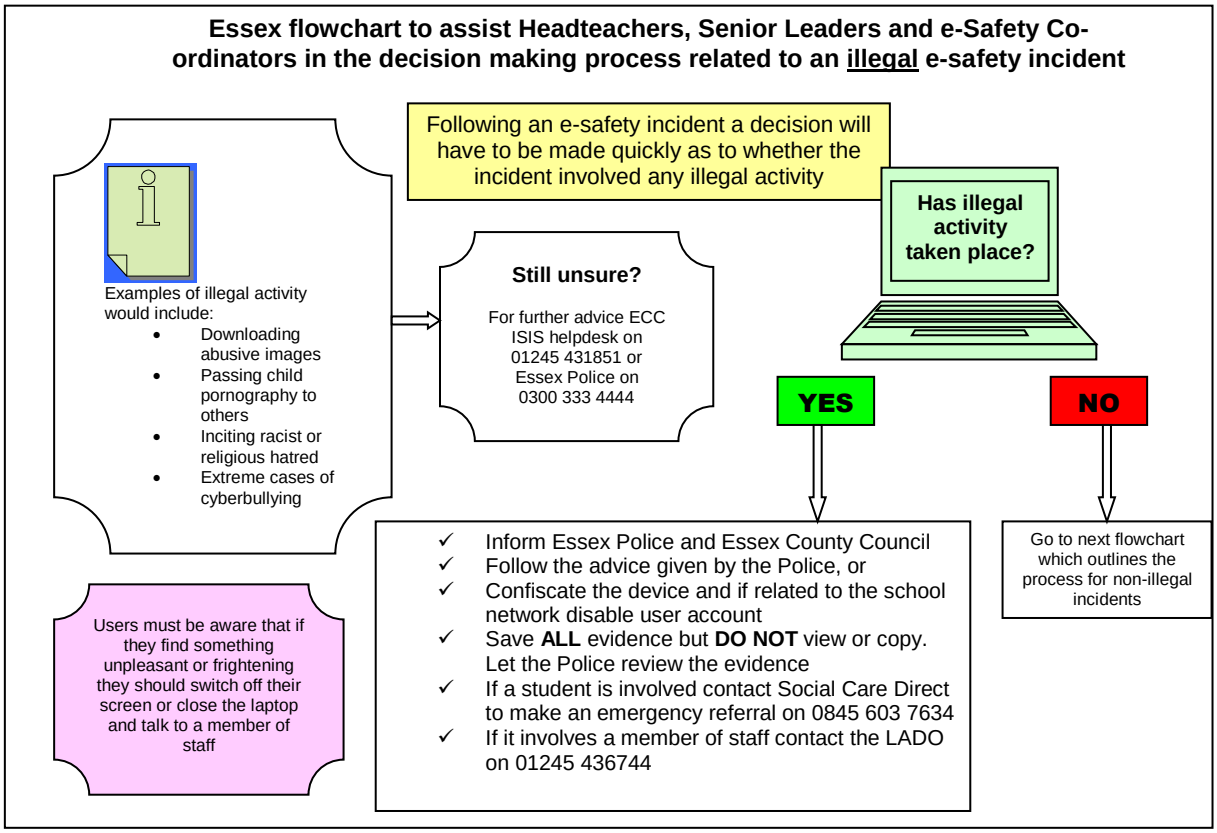
Misuse and Infringements

Complaints
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Head of Year. Incidents are logged and the **Essex Flowcharts for Managing an eSafety Incident** is followed.

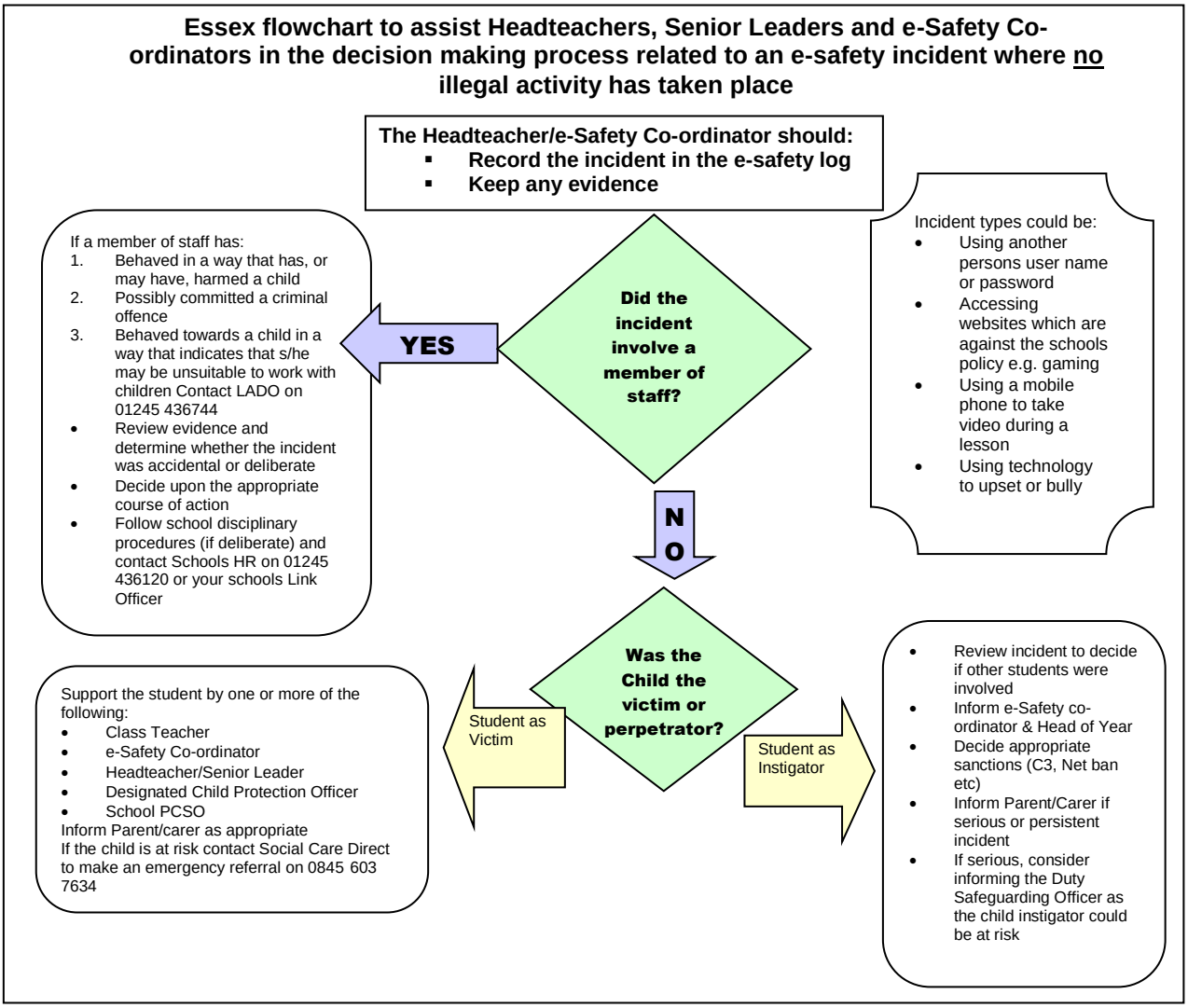
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any staff user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Deliberate access to inappropriate materials by any student user will lead to the incident being logged by the eSafety co-ordinator or Head of Year, depending on the seriousness of the offence; investigation, immediate suspension for the school network, possibly leading to detention, exclusion and involvement of parents with involvement of police for very serious offences (see flowchart)

- Users are made aware of sanctions relating to the misuse or misconduct by means of tutor time messages and in ICT lessons. Users are reminded that they are being monitored by means of an onscreen reminder every time that they log onto the school system



Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where <u>no</u> illegal activity has taken place



Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **school internet, intranet and extranet** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff should preview any recommended sites before use
- Raw image searches are discouraged when working with students
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and students and how this is disseminated.

Infrastucture

- Great Baddow High school has a monitoring solution where web-based activity is monitored and recorded
- School internet access is controlled on-premises through the schools unified threat management gateway. For further information relating to filtering please email the Network Management Team filtering@gbhs.co.uk with any questions or requests to block/unblock sites
- Great Baddow High school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site the incident should be reported immediately to the e-safety coordinator or classroom teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.

- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from their Computer Science teacher or the network managers

- If there are any issues related to viruses or anti-virus software, the network manager should be informed via email to nm@gbhs.co.uk

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to students within school unless teacher directed during curriculum time
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly promote eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

- Parents/ carers are expected to sign the Acceptable Use Policy agreement containing the following statement

    - **Students must not distribute or import from data stick, disk or other portable storage device materials to others which could be classed as offensive, obscene, bullying or damaging;**

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training links

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User accounts and passwords for staff and students who have left the School are disabled within 3 months and archived within 24 months

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From *Year 7* they are also expected to use a personal password and keep it private
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 5.00pm. After this time staff can log back in to the network and it is their responsibility to ensure that equipment is logged-off and shut down.
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the network manager and all staff and students are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

Further advice available http://www.itgovernance.co.uk/

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your line manager or the head teacher
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience – see also Social Media Policy
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Take particular care when cloning your machine onto a whiteboard for classroom display
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. ECC guidance can be found: http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others without permission.

Consent of Adults Who Work at the School

- Photographs of staff are required for identification purposes and for use on entry passes. Permission to use images of staff elsewhere in the school is sought on induction and a copy is located in the personnel file

Publishing Student's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. in which case the school should be informed of any change of permissions

Parents/ carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published by the school.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Authorised personnel only may upload student work to the internet.

Further information relating to issues associated with School websites and the safe use of images in Essex schools on the Essex Schools Infolink http://esi.essexcc.gov.uk

---

Storage of Images

- Images/ films of children are stored on the school's network
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform
- Staff have the responsibility of deleting the images when they are no longer required, or the student has left the school

---

Webcams and CCTV

- The school uses CCTV for security and safety. Authorised personnel only have access to this. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance
  http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

For further information relating to webcams
http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Anti_Bullying/antibullying_cyberbullying_DCSF_sept07.pdf

---

Video Conferencing

- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- Approval from the Headteacher or deputy is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information relating to Video Conferencing
https://www.education.gov.uk/publications/standard/_arc_Subjects/Page11/15007

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment to the network manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for

insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

---

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- This technology may be used, however for educational purposes, as mutually agreed with the teacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite

visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device should be used to conduct school business outside of school

---

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media' - Page - 11 -7

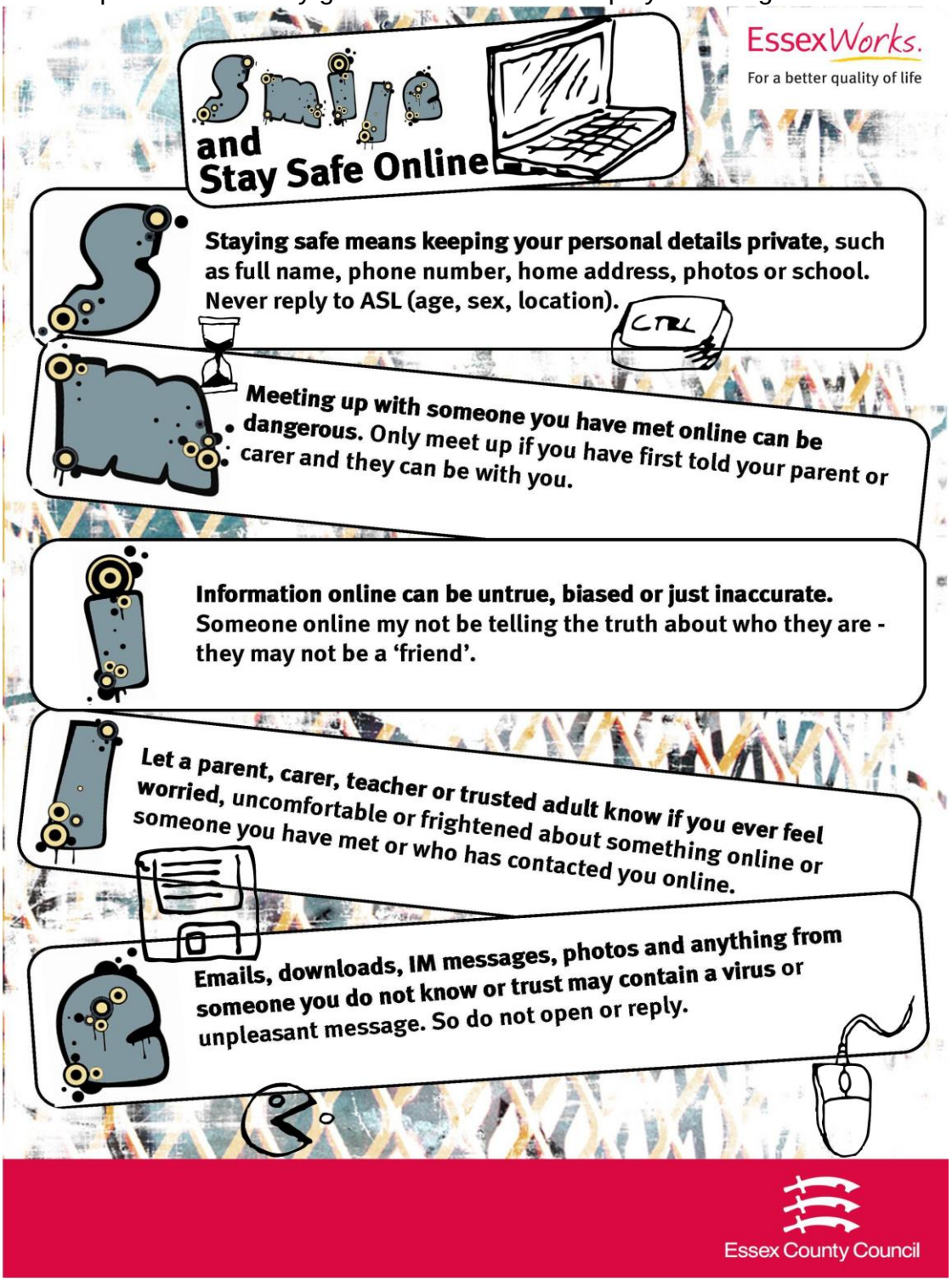
- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Newly installed servers holding personal data should be protected, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software
- Always keep servers in a locked and secure environment
- Limit access rights to ensure the integrity of the standard build
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Records should be kept of when and which patches have been applied
- Ensure that web browsers and other web based applications are operated at a minimum of 256 BIT cipher strength

Smile and Stay Safe Poster

An example of the eSafety guidelines which are displayed throughout the school



Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing of the data.

Telephone Services

- You may make or receive personal telephone calls provided:

1. They are infrequent, kept as brief as possible and do not cause annoyance to others
2. They are not for profit or to premium rate services
3. They conform to this and other relevant ECC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times

---

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services
- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

Writing and Reviewing this Policy

Staff and Student Involvement in Policy Creation

- Staff and students have been involved in making/ reviewing the Policy for ICT Acceptable Use through the ICT Strategy group and school council

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed annually and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.legislation.gov.uk/ukpga/1998/29/contents

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making 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.

http://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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.

http://www.legislation.gov.uk/ukpga/2006/1/contents

Sexual Offences Act 2003

The new grooming offence 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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

http://www.legislation.gov.uk/ukpga/2003/42/contents

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

http://www.legislation.gov.uk/ukpga/2003/21/contents

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 another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

http://www.legislation.gov.uk/ukpga/1990/18/contents

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) 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.

http://www.legislation.gov.uk/ukpga/1988/27/contents

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. 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. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them 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.

http://www.legislation.gov.uk/ukpga/1988/48/contents

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.

http://www.legislation.gov.uk/ukpga/1986/64/contents

Protection of Children Act 1978 (Section 1)

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). A person convicted of such an offence may face up to 10 years in prison.

http://www.legislation.gov.uk/ukpga/1978/37/contents

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

1964 - http://www.legislation.gov.uk/ukpga/1964/74/contents
1959 - http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents

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.

http://www.legislation.gov.uk/ukpga/1997/40/contents

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

The Freedom of Information Act 200

http://www.legislation.gov.uk/ukpga/2000/36/contents

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx