EssexWorks.
For a better quality of life

NOTLEY HIGH SCHOOL & BRAINTREE SIXTH FORM

Based on Model Policies for Schools

E-safety and Data Security

(Including Acceptable Use Agreements)

Developed by:	**ICT Strategy Group**
Author:	**Mr R Newman, Senior Deputy Headteacher**
Date of issue:	**July 2013**
Review date:	**July 2015**

Senior Information Risk Owners (SIROs) – Mr R Newman, Mrs R Kelly

Information Asses Owners (IAO) – Mrs V Homan-Smith, Mr M Fuller, Mrs T Dynowska

E-safety Co-ordinator – Mrs V Homan-Smith

Essex County Council

CONTENTS

Acknowledgement

We acknowledge and thank Hertfordshire County Council for their help in producing this model policy.

This policy is intended for staff and student use.

This policy should be issued to all personnel, including governors and students, involved in the working of the school.

The Acceptable Use of ICT Agreement should be issued to the appropriate user for signature and collated by a designated member of staff.

All persons, including governors and students, who join the establishment mid-year are provided with the policy and agreement.

Introduction

ICT in the 21st century is an essential resource to support teaching and learning, 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
- Podcasting
- Video Broadcasting
- 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 Notley High School & Braintree Sixth Form we understand the responsibility to educate our students on e-safety 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 on to school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

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.

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 procedures.

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 school's Senior Information Risk Owners (SIROs) or E-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access secure ID tokens and PINs), virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SIROs.

The school's SIROs are the Senior Deputy Headteacher and the Deputy Headteacher with strategic oversight of Behaviour & Safety. The school's E-safety Co-ordinator is the ICT& Business Faculty Leader.

See flowcharts on page 24 for dealing with both illegal and non-illegal incidents.

Acceptable Use Agreement: Students - Secondary

Secondary Student Acceptable Use Agreement / E-safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.

- I will not download or install software on school technologies.

- I will only log on to the school network/learning platform with my own user name and password.

- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.

- I will only use my school e-mail address.

- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.

- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.

- Images of students will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network if parents/carers opt out of this by informing the school in writing.

- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.

- I will respect the privacy and ownership of others' work on-line at all times.

- I will not attempt to bypass the internet filtering system.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

EssexWorks.
For a better quality of life

Dear Parent/Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school.   We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of e-safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form tutor or Mrs V Homan-Smith, the school's E-safety Co-ordinator.

Please return the bottom section of this form to school for filing.

This Acceptable Use Agreement is a summary of our E-safety Policy which is available in full on our school website or by contacting Mrs P Ferady, Headteacher's secretary.

Yours faithfully,

Mr R Newman
Senior Deputy Headteacher

---✂

Student and Parent/Carer signature

We have discussed this document and ………………………………………........(student name) agrees to follow the e-safety rules and to support the safe and responsible use of ICT at Notley High School & Braintree Sixth Form.

Parent/Carer Signature ………………………………………………….

Student Signature………………………………………………………….

Form ………………………………… Date ………………………………

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs V Homan-Smith, E-safety Co-ordinator or with Mr R Newman or Mrs R Kelly, the school's Senior Information Risk Owners.

- I will only use the school's e-mail/internet/intranet/learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software without permission of the school's ICT Network Manager (Mr M Fuller).
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of staff will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside if staff members opt out of this by informing the Headteacher in writing.
- Images of students will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network if parents/carers opt out of this by informing the school in writing.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that the current value of laptops and mobile devices brings them below the school's insurance excess levels. Therefore equipment issued to me will be at my own risk whilst off-site either in transit or at my residence. It is expected that due care and attention will be taken to keep school-issued equipment secure and in good order.

This Acceptable Use Agreement is a summary of our E-safety Policy which is available in full on request

User Signature:
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….………………….………………….…… Date ………………………………………….

Full Name ………………………………….. (printed) Role …………………...……………………

Computer Viruses

- All files downloaded from the internet, received via e-mail or on removable media (e.g. USB, 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 the IT Network Team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT Network Team immediately. The ICT Network Team will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously and it follows Department for Education guidance.

Other helpful documentation includes:

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

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 (SIMS), 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.
- The school have identified Senior Information Risk Owners (SIROs) and Asset Information Owners (AIOs).
- 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 school's fax procedures overleaf (based on Safe Haven Fax Procedures):

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;
- check that it has been received by the correct recipient;
- wait for the original to process and remove it from the fax machine;
- 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 the school to secure data and so reduce the risk of security incidents.
- 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.
- The protective mark should be in bold capital letters within the header and footer of each page of a document.
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset.

Senior Information Risk Owners (SIROs)

SIROs are senior members of staff who are familiar with information risks and the school's response. Typically, the SIROs should be member of the senior leadership team and have the following responsibilities:

- they own the Information Risk Policy and risk assessment;
- they appoint the Information Asset Owners (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.

The SIROs in this school are Mr R Newman (Senior Deputy Headteacher) and Mrs R Kelly (Deputy Headteacher).

Information Asset Owners (IAOs)

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. Schools should identify Information Asset Owners. The school's IAOs are Mrs V Homan-Smith (E-safety Co-ordinator), Mr M Fuller (ICT Network Manager) and Mrs T Dynowska (SIMS & Data Manager).

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 of.

As a result, 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 secure 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.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

- All redundant ICT equipment that may have held personal data will have the storage media over-written multiple times to ensure the data is irretrievably destroyed, or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
  Data Protection Act 1998
  http://www.ico.gov.uk/what_we_cover/data_protection.aspx
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

- The school's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of e.g. waste, gift, sale
  - Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency website

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 e-mail 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 institution'. 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/carers or students are advised to cc. their line manager or other appropriate person.

- Students should only use school approved accounts on the school system and only 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 should 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.

- The forwarding of chain letters is not permitted in school.

- 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 E-safety Co-ordinator/Line Manager) if they receive an offensive e-mail.

- Students are introduced to e-mail as part of the ICT curriculum.

- 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 business 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.

- 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.

- Activate your ‘out-of-office’ notification when away for extended periods.

- Use the ‘Delegation’ facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if appropriate to do so).

- Never open attachments from an untrusted source; consult the ICT Network Team first.

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

E-mailing Personal, Sensitive, Confidential or Classified Information

- The school has an email-based encryption method which is used by key staff to send personal, sensitive, confidential or classified information.

- Where an encrypted e-mail is used to transmit such data:

  – Obtain express consent from the school’s SIROs to provide the information by e-mail.
  – Exercise caution when sending the e-mail and follow the processes in place.
  – Do not identify such information in the subject line of any e-mail.

Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the school's e-safety 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 e-safety issues.

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

E-safety

E-safety - Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety Co-ordinator in this school is Mrs V Homan-Smith, supported by Mr R Newman and Mrs R Kelly who have been designated this role as members of the senior leadership team. All members of the school community have been made aware of who holds these posts. It is the role of the E-safety Co-ordinator to keep abreast of current issues and guidance through organisations such ECC, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior management and governors are updated by the Headteacher/E-safety 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 school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHEe.

E-safety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT lessons (as seen in schemes of learning).
- The school supports the annual Safer Internet Day in February each year to promote e-safety.
- Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety 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.

- Students are taught to critically evaluate materials and learn good searching skills via the ICT curriculum.

E-safety Skills Development for Staff

- Our staff receive regular information and training on e-safety issues.
- New staff receive information on the school's acceptable use guidance as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety 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 e-safety activities and awareness within their curriculum areas.

Managing the School E-safety Messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-safety Policy will be introduced to the students at the start of each school year.
- E-safety information will be prominently displayed on the information screens around the school. Assemblies will focus on e-safety on a regular basis.

Incident Reporting, E-safety 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 SIROs or E-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the school's Senior Information Risk Owners.

E-safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident following school policy.

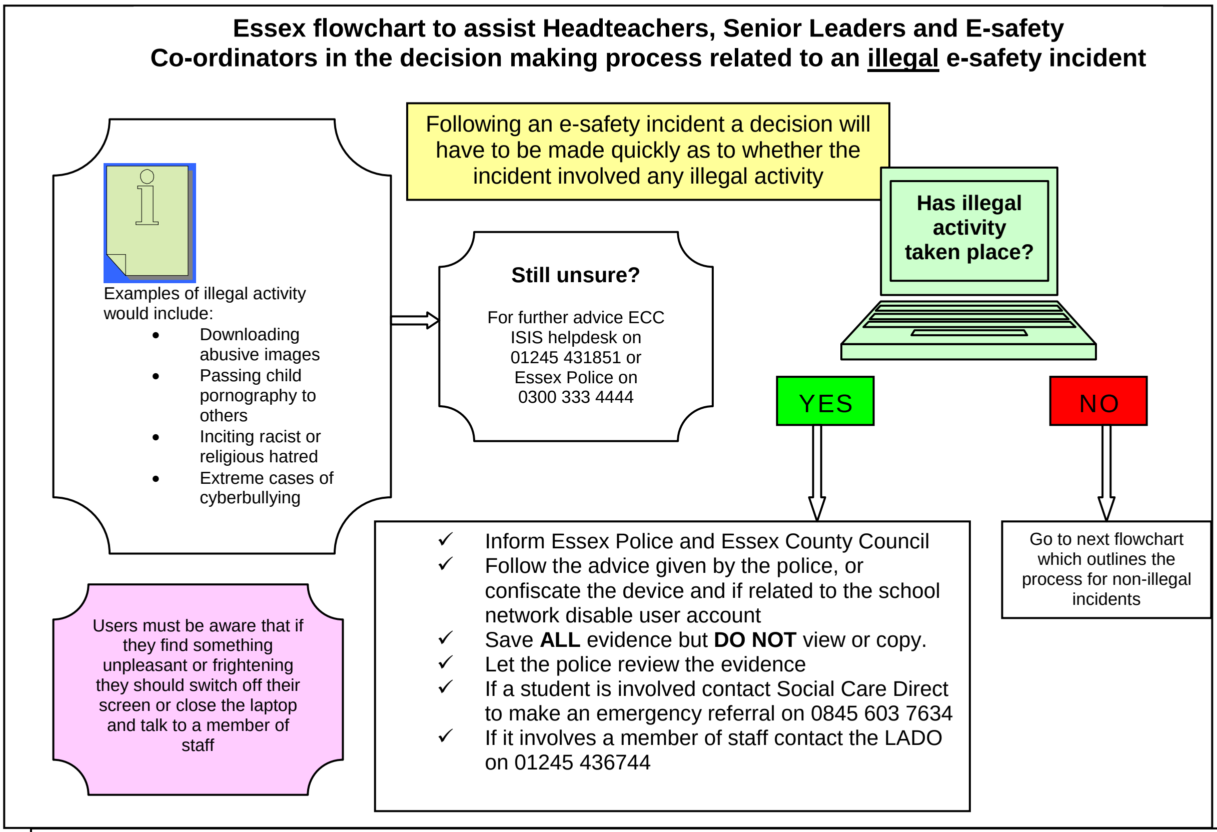
Misuse and Infringements

Complaints

Complaints and/or issues relating to e-safety should be made to the E-safety Co-ordinator or Headteacher. Incidents should be logged and the **Essex Flowcharts for Managing an E-safety Incident** should be considered to support any next course of action.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the IT Network Team.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety Co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).
- Users are made aware of sanctions relating to the misuse or misconduct.



Essex flowchart to assist Headteachers, Senior Leaders and E-safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying

Still unsure?

For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

Has illegal activity taken place?

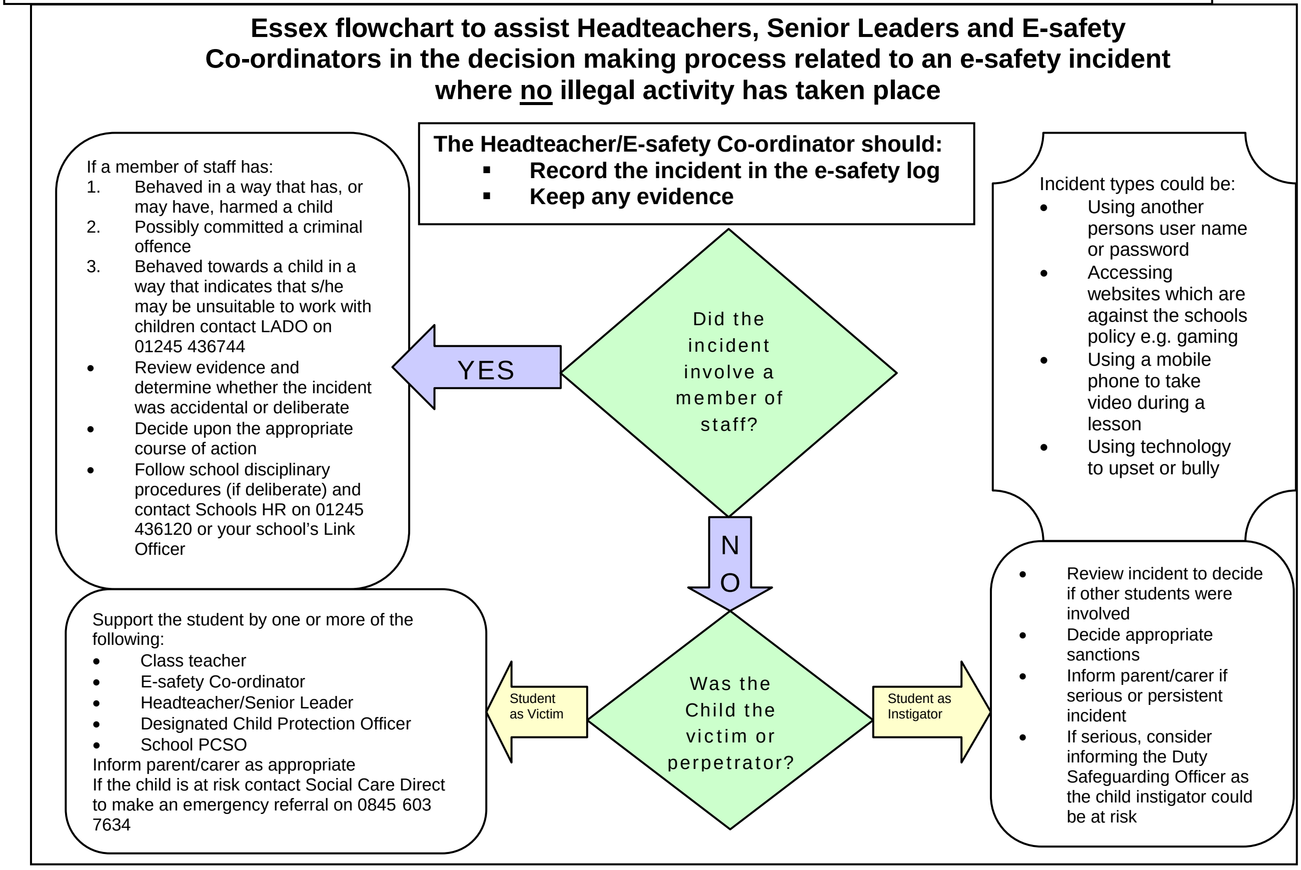
YES

NO

- ✓ Inform Essex Police and Essex County Council
- ✓ Follow the advice given by the police, or confiscate the device and if related to the school network disable user account
- ✓ Save **ALL** evidence but **DO NOT** view or copy.
- ✓ Let the police review the evidence
- ✓ If a student is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
- ✓ If it involves a member of staff contact the LADO on 01245 436744

Go to next flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff



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

The Headteacher/E-safety Co-ordinator should:

- **Record the incident in the e-safety log**
- **Keep any evidence**

Did the incident involve a member of staff?

YES

If a member of staff has:

1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children contact LADO on 01245 436744

- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your school's Link Officer

Incident types could be:

- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

NO

Was the Child the victim or perpetrator?

Student as Victim

Support the student by one or more of the following:

- Class teacher
- E-safety Co-ordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- School PCSO

Inform parent/carer as appropriate

If the child is at risk contact Social Care Direct to make an emergency referral on 0845 603 7634

Student as Instigator

- Review incident to decide if other students were involved
- Decide appropriate sanctions
- Inform parent/carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

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 **Essex Grid for Learning** (EGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Students have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology. Unsupervised access may take place for Sixth Form students.
- Staff will preview any recommended sites before use.
- If internet research is set for home learning, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work, especially for students in Years 7-9.
- 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.
- Online gambling or gaming is not allowed.

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

Infrastucture

- School internet access is controlled through the school's own web filtering service. For further information relating to filtering please contact itsupport@notleyhigh.com
- Notley High School & Braintree Sixth Form 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 e-mail and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety Co-ordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the IT 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 IT Network Team'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 subject teacher/IT Network Team.
- If there are any issues related to viruses or anti-virus software, the IT Network Team should be informed.

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 Years 7-11 students within school.

- 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, e-mail 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 school’s Virtual Learning Environment or other systems approved by the Headteacher.

Parent/Carer Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and also to be aware of their responsibilities. We provide e-safety information for 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 wish to opt out to images of their child being taken/used in the public domain (e.g. on school website). Sixth Form students are able to make this decision themselves.

- Parents/carers are expected to sign a Home-School Agreement containing reference to e-safety. Sixth Form students are able to sign this agreement themselves.

- The school disseminates information to parents/carers relating to e-safety where appropriate in the form of:
    - Information evenings
    - Website postings
    - Newsletter items

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 log on. Do not include passwords in any automated log on procedures.
- Staff should change temporary passwords at first log on.
- 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 characters as directed by the ICT Network Team.
- User ID and passwords for staff and students who have left the school are removed from the system as soon as possible and within 10 working days.

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Network 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 log-in username. 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 the school network, SIMS/Virtual Learning Environment, including ensuring that passwords are not shared and are changed when requested to do so by the IT Network Team. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the Virtual Learning Environment to the browser/cache options (shared or private computer).

- In our school, all ICT password policies are the responsibility of the ICT Strategy Group and all staff and students are expected to comply with the policies at all times.

Zombie Accounts

Zombie accounts refer 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 unauthorised access.

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

Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009. Schools may wish to sign up to this promise which is shown below.

The personal information promise is:

The ICT Strategy Group on behalf of Notley High School & Braintree Sixth Form promise that we will:

- value the personal information entrusted to us and make sure we respect that trust;
- go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
- consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- be open with individuals about how we use their information and who we give it to;
- make it easy for individuals to access and correct their personal information;
- keep personal information to the minimum necessary and delete it when we no longer need it;
- have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
- provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
- put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
- regularly check that we are living up to our promises and report on how we are doing.

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 manager.
- 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.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- 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 confidential and do not disclose them to anyone.
- 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/carers (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 permission of the Headteacher, images can be taken provided they are used solely for educational purposes, transferred to the school's network and deleted from the staff device.
- Students are not permitted to routinely use personal digital equipment, including mobile phones and cameras, to record images of other students and staff, this includes when on field trips. However with the permission of the Headteacher and students/staff involved, images can be taken and used for educational purposes.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Student Images and Work

On a child's entry to the school, all parents/carers will be informed that their child's work/photos can be used in the following ways unless they expressly opt out of this:

- on the school website;
- on the school's Virtual Learning Environment;
- 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;
- in the local/national media/press releases sent to the press.

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.

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.

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.

Only the Web Manager has authority to upload to the site or other staff with delegated responsibility from the senior team.

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 only.
- Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks, mobile phones) without the express permission of the Headteacher.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the senior team, student services, the IT Network Team and Media Manager. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes and never using images of children or adults.
- 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

- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in

video conferences with end-points outside of the school.

- 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.
- The school keeps a record of video conferences, including date, time and participants.
- 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 third 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.

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.

- The school logs ICT equipment issued to staff and records 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. The IT Network Team will provide support as required.

- 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 PC/other devices accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment cannot be used on the school network unless with permission from the IT Network Team.

- On termination of employment, resignation or transfer, return all ICT equipment to the ICT Network Team. You must also provide details of all your system log ons 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 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, tablets, smartphones 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 IT Network Team and fully licensed.

- 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, gaming devices, mobile and smartphones 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 smartphones)

- 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 in Years 7-11 are allowed to bring personal mobile devices/phones to school but must not use them between 8.30am and 3.20pm unless they have permission to do so from a member of staff. At all times the device must be switched onto silent or turned off and be out of sight. If devices are seen during the day, they will be confiscated by staff until the end of the school day. Separate protocols exist for Sixth Form students.

- When this technology is permitted to be used for educational purposes, as mutually agreed with the Headteacher, 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 smartphones)

- 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 tablets for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, it should be used to conduct school business appropriately.

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’.

- Only use recommended removable media;
- Store all removable media securely;
- Removable media must be disposed of securely by the IT Network Team.

Servers

- Servers are kept 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.
- Back up tapes should be encrypted by appropriate software.
- 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.

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 log ons, 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 log off 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 into disrepute. This includes, but is not limited to, jokes, chain letters, files, e-mails, 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 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.

- 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.

Policy Review Procedures

There will be an on-going opportunity for staff to discuss with the E-safety Co-ordinator any issue of e-safety that concerns them.

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

This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning.

The policy will be further amended as necessary if new technologies are adopted by the school.

It is the responsibility of the ICT Strategy Group to review and update this policy.

Current Legislation

Acts Relating to Monitoring of Staff E-mail

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.hmso.gov.uk/acts/acts1998/19980029.htm

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.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to E-safety

Racial and Religious Hatred Act 2006

It is 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.

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.

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.

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.

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.

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.

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.

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.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 200

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