Fairhouse Primary School

eSafety and Data Security

Guidance Policies for ICT Acceptable Use

Department: SCF Information Governance

Date of issue: Summer 2016  e-safety Co-ordinator – Maggie Elfenich
To be reviewed: Summer 2017  SIRO – Jenny McCutcheon
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Monitoring</td>
<td>6</td>
</tr>
<tr>
<td>Breaches</td>
<td>7</td>
</tr>
<tr>
<td>Incident Reporting</td>
<td>7</td>
</tr>
<tr>
<td>Acceptable Use Agreement: Pupils - Primary</td>
<td>10</td>
</tr>
<tr>
<td>Acceptable Use Agreement: Pupils - Secondary</td>
<td>10</td>
</tr>
<tr>
<td>Acceptable Use Agreement: Staff, Governors And Visitors</td>
<td>12</td>
</tr>
<tr>
<td>Computer Viruses</td>
<td>13</td>
</tr>
<tr>
<td>Data Security</td>
<td>13</td>
</tr>
<tr>
<td>Security</td>
<td>14</td>
</tr>
<tr>
<td>Impact Levels and Protective Marking</td>
<td>15</td>
</tr>
<tr>
<td>Senior Information Risk Owner (SIRO)</td>
<td>15</td>
</tr>
<tr>
<td>Information Asset Owner (IAO)</td>
<td>17</td>
</tr>
<tr>
<td>Disposal Of Redundant Ict Equipment Policy</td>
<td>17</td>
</tr>
<tr>
<td>E-mail</td>
<td>19</td>
</tr>
<tr>
<td>Managing e-Mail</td>
<td>19</td>
</tr>
<tr>
<td>Sending e-Mails</td>
<td>20</td>
</tr>
<tr>
<td>Receiving e-Mails</td>
<td>21</td>
</tr>
<tr>
<td>e-mailing Personal, Sensitive, Confidential or Classified Information</td>
<td>21</td>
</tr>
<tr>
<td>Future Developments</td>
<td>22</td>
</tr>
<tr>
<td>Equal Opportunities</td>
<td>23</td>
</tr>
<tr>
<td>Pupils with Additional Needs</td>
<td>23</td>
</tr>
<tr>
<td>Esafety</td>
<td>24</td>
</tr>
<tr>
<td>eSafety - Roles and Responsibilities</td>
<td>24</td>
</tr>
<tr>
<td>eSafety in the Curriculum</td>
<td>24</td>
</tr>
<tr>
<td>eSafety Skills Development for Staff</td>
<td>25</td>
</tr>
<tr>
<td>Managing the School eSafety Messages</td>
<td>25</td>
</tr>
<tr>
<td>incident Reporting, Esafety Incident Log &amp; Infringements</td>
<td>26</td>
</tr>
<tr>
<td>Incident Reporting</td>
<td>26</td>
</tr>
<tr>
<td>eSafety Incident Log</td>
<td>26</td>
</tr>
<tr>
<td>Misuse and Infringements</td>
<td>27</td>
</tr>
<tr>
<td>Flowcharts for Managing an eSafety Incident</td>
<td>27</td>
</tr>
<tr>
<td>internet Access</td>
<td>29</td>
</tr>
</tbody>
</table>
Acknowledgement

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

ICT in the 21\textsuperscript{st} 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
- 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 Fairhouse Primary School we understand the responsibility to educate our pupils 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 your 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 pupils) 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 pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).
Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Essex County Council (ECC) staff.
**Breaches**

A breach or suspected breach of policy by a School employee, contractor or pupil 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 school’s Senior Information Risk Owner (SIRO) 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.
Pupil Agreement/eSafety Rules

- I will only use ICT in school for school purposes.

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

- I will only open e-mail attachments from people I know, or who my teacher has approved.

- I will not tell other people my ICT passwords.

- I will only open/delete my own files.

- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

- I will not give out my own details such as my name, phone number or home address.

- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

- I will be responsible for my behaviour/equipment when using ICT because I know that these rules are to keep me safe.

- I know that the use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

- I will not change setting on any ICT equipment.

- I will turn off my mobile phone and give it to my teacher at the start of the day.

Pupil’s Name ............................................................................................................. Date ..............................................
**Parent Agreement**

The following box is part of our Admission Forms, which parent/carers sign to confirm their agreement.

**Internet Permission**
I grant permission for my child to use the internet in school. I understand that pupils will be held accountable for their own actions. I understand that some materials on the internet may be inappropriate for use in school, such as game sites. Therefore, there will be restricted access to some sites.

Parent/Carer Signature .................................................................
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 Maggie Elfenich, Fairhouse Primary school eSafety coordinator or Mrs Jennifer McCutcheon, Fairhouse Primary School Senior Information Risk Owner.

- I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head 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 pupils 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 pupils.
- 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 Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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. (See Social Media Policy.)
- I will support and promote the school’s e-Safety and Data Security policies and help pupils 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.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on our website.

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)
Job title ............................................................................................................
Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, external hard drive, 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.
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/pupilsupport/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 have read 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 Protect, although some data e.g. Child Protection data, should be classed as Restricted.
• Protect/Restrict and caveat classifications that schools may use are;
  - PROTECT – PERSONAL e.g. personal information about an individual
  - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
  - PROTECT – LOCSEN e.g. for local sensitive information
  - PROTECT – STAFF e.g. Organisational staff only
  - RESTRICTED e.g. sensitive personal information about an individual
• 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
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

---

**Senior Information Risk Owner (SIRO)**

The SIRO is a senior member of staff who is familiar with information risks and the school’s response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- 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 SIRO in this school is (name).

---

**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. Schools should identify an Information Asset Owner. For example, the school’s Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

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, pupil 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 IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

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.
Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off 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 overwritten 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
  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 & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be overwritten 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 web site**

Introduction


The Waste Electrical and Electronic Equipment Regulations 2006


The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007


**Information Commissioner website**

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

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

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. 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 pupil based, within school or international. We recognise that pupils 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, pupils 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 pupils, 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 pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils 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 pupils have use of their email. This can only be used within the school community.

• All pupil 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.

• Pupils 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.

• Pupils are introduced to e-mail as part of the Computing 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.

**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
- 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 available within your software)
- 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:

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

Future Developments

There is currently a review taking place on the way e-mails are sent whereby all such 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 pupil, 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

Pupils with Additional Needs

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

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

Where a pupil 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 *(name)* who has been designated this role as a member of the senior leadership team. 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 as 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 pupils, 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/pupil 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 pupils 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 Computing / PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils 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
- Pupils are taught about copyright and respecting other people’s information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if
they are affected by any form of online bullying. Pupils 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

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

---

**eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety issues in the form of staff meetings
- The staff training programme is ongoing
- New staff receive information on the school’s acceptable use policy as part of their induction
- 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

---

**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 pupils at the start of each school year
- eSafety posters 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 - 15 -.

eSafety Incident Log

eSafety incidents are recorded on an eSafety Incident form.

Fairhouse Primary School

INCIDENT REPORT (E-SAFTY)

Reference________________________________  Date________________________

Incident

Witnessed by________________________________

Consequence

Reported by________________________________

Action Taken (if required)

Head Teacher’s Signature_________________________  Date________________________
Misuse and Infringements

Complaints
Complaints and/or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the Essex Flowcharts for Managing an eSafety Incident should be 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 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)
- Users are made aware of sanctions relating to the misuse or misconduct through staff training
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.

**Has illegal activity taken place?**

- **YES**
  - 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 pupil 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

- **NO**
  - 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**

**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

---

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

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 schools Link Officer

Support the pupil 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

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

Did the incident involve a member of staff?

- **YES**
  - Review incident to decide if other pupils 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

- **NO**
  - Pupil as Victim
  - Pupil as Instigator

Was the child the victim or perpetrator?

- Pupil as Victim
- Pupil as Instigator
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

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- 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 pupils and how this is disseminated.

Infrastructure

- Essex County Council has a monitoring solution via the Essex Grid for Learning where web-based activity is monitored and recorded
School internet access is controlled through the LA’s web filtering service. For further information relating to filtering please email essexcc-servicedesk.sen.uk@siemens-enterprise.com with any questions or requests to block/unblock sites.


Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

The school does not allow pupils access to internet logs.

The school uses management control tools for controlling and monitoring workstations.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or 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.

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission.

If there are any issues related to viruses or anti-virus software, the network manager 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 pupils 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 pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils 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
- Pupils 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 pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils 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 pupils using the school email 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 consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by commenting on Parents Evening Surveys.

- 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 a Home School agreement containing the following statement or similar:

  → We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.

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

  o Information and celebration evenings
  o Posters
  o Website
  o 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 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 ID and passwords for staff and pupils who have left the School are removed from the system.

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 pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils 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.
- Pupils 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.

- 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 Jenny McCutcheon and all staff and pupils 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/](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:

I (name and title), on behalf of (name of organisation) promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. 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;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. 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;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing

More information available -


To view the promise

To sign up to the Promise
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/personal_information_promise.aspx  go down to the bottom of the page
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 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 pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, 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

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, 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 pupil’s device

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 Pupil’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

- 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.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils’ names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils’ 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.

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
- Pupils 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 pupils within the confines of the school network/ Learning Platform
- Teachers have the responsibility of deleting the images when they are no longer required, or the pupil has left the school

**Webcams and CCTV**

- We do not use publicly accessible webcams in school

---

**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 pupils are supervised by a member of staff when video conferencing

• All pupils 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.

• Approval from the Headteacher 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
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your 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
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 pupil or parent/carer using their personal device.
- Pupils and staff 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 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 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 may 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 - 36 -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 encrypted, 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
- 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
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength
Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

- Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

- Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

- Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a ‘friend’.

- Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

- Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.
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

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

**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 Pupil Involvement in Policy Creation

Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use.

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 every (12) months 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.

This policy has been read, amended and approved by the staff, head teacher and governors.
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.


*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.


*Human Rights Act 1998*


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.


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.


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**
