A member of HART SCHOOLS TRUST

ROEBUCK ACADEMY
Dream-Believe-Achieve

E-Safety Policy

Introduction

ICT in the 21st Century is seen as 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
Apps
E-mail, Instant Messaging and chat rooms
Social Media, including Facebook and Twitter
Mobile/ Smart phones with text, video and/ or web functionality
Other mobile devices including tablets and gaming devices
Online Games
Learning Platforms and Virtual Learning Environments
Blogs and Wikis
Podcasting
Video sharing
Downloading
On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements (13 years in most cases).

At Roebuck Academy, we understand the responsibility to educate our pupils 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.

Everybody in the school community 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, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, 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 and other mobile devices).

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, video 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.
All internet activity is logged by the school's internet provider. These logs may be monitored by that provider (e.g. Herts for Learning Ltd).

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. For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.
The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.
The data protection powers of the Information Commissioner's Office are to:

Conduct assessments to check organisations are complying with the Act;

Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

Prosecute those who commit criminal offences under the Act;

Conduct audits to assess whether organisations' processing of personal data follows good practice,

Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

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 relevant responsible person. 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 the relevant responsible person. The relevant responsible individuals in the school are as follows: Lynsey Young and Andy Mari.

Please refer to the relevant section on Incident Reporting, E-Safety Incident Log & Infringements.

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

ICT and the related technologies such as email, 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 the school Computing coordinator or the Headteacher.

- 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 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 pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) 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 of software without permission of the E-Safety coordinator.
- 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 in line with school policy. No images will be used, or distributed outside the school network, if the school has been notified of this wish by parents/carers.
- 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 Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- 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 Computing policy (including E-Safety) 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.

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

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

Full Name ……………………………….. (printed)

Job Title ……………………………………………………………

Staff Professional Responsibilities

The HSCB, (Hertfordshire Safeguarding Children Board), E-Safety subgroup group have produced a clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment. 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.
- The accessing and appropriate use of school data is something that the school takes very seriously.

The Local Authority guidance documents listed below:

- HGfL: School Admin: School Office: Data Protection and Freedom of Information
- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts
- Security
-
- Security
- The school gives relevant staff access to its Management Information System, with a unique username 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 SITSS website concerning 'Safe Handling of Data' (available on the grid at http:// www.thegrid.org.uk/info/dataprotection/index.shtml#securedata).

Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/).

- 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.
-
- Protective Marking of Official Information
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.
- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion. Existing information does not need to be remarked. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE' Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.
- Staff

Protective Marking of Official Information

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes. There is no requirement to mark routine OFFICIAL information. Optional descriptors can be used to distinguish specific type of information. Use of descriptors is at an organisation's discretion. Existing information does not need to be remarked. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response.

- They lead on the information risk policy and risk assessment
- They advise school staff on appropriate use of school technology
- 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 relevant responsible staff members in their role.

‘

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the school:

- What information is held, and for what purposes?
- What information needs to be protected, how information will be amended or added to over time?
- Who has access to the data and why? How is information is retained and disposed of?

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements.
However, it should be clear to all staff that 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 of through an authorised agency. 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.environment-agency.gov.uk/business/topics/waste/32084.aspx
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
Sometimes called a SIRO, there should be a member of the senior leadership team who has the following responsibilities Data Protection Act 1998
https://ico.org.uk/for-organisations/education/
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 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 web site
2007
Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Information Commissioner website
https://ico.org.uk/
Data Protection Act – data protection guide, including the 8 principles
https://ico.org.uk/for-organisations/education/
PC Disposal – SITSS Information
http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal
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 how to behave responsible online.

Managing e-mail

The school gives all staff and governors their own e-mail account to use for all school business as a work based tool.

- This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Staff and governors should use their school email for all professional communication.
- 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 line manager.
- 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 pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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 or upsetting e-mail.
- Staff must inform (the E-Safety
- Leader or line manager) if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing Programme of Study.
- 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

Use your own school e-mail account so that you are clearly identified as the originator of a message.
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.
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.
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

Where your conclusion is that e-mail must be used to transmit such data:
Either: Obtain express consent from your manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect. See http://www.thegrid.org.uk/info/ dataprotection/#securedata
- 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 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).
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt.
- OR: Use Hertsfx or Schools fx, Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely http://www.thegrid.org.uk/eservices/ schoolsfx.shtml

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil 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 - Roles and Responsibilities

As E-Safety 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 E-Safety Leader in this school is Andy Mari who has been designated this role as Computing lead. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety Leader to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ E-Safety Leader and all governors have an understanding of the issues and strategies at our school a member of the senior leadership team 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 PSHCE.

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 pupils 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 lessons computing/PSHE lessons.
The school provides opportunities within a range of curriculum areas to teach about safety
Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety 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, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate 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 Cybermentors, 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.

E-Safety Skills Development for Staff

Our staff receive regular information and training on E-Safety and how they can promote the 'Stay Safe' online messages in the form of staff meetings and updates. Details of the ongoing staff training programme can be found in Head teacher's office and in staff meeting minutes. New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of their 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 E-Safety Leader). All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

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 pupils at the start of each school year.**
- E-Safety posters will be prominently displayed.
- **The key E-Safety advice will be promoted widely through school displays, newsletters,** class activities and so on.

We may participate in Safer Internet Day each year.

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 relevant responsible person or E-Safety Leader. 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 Information Asset Owner.

E-Safety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.
This can be downloaded http://www.thegrid.org.uk/eservices/safety/incident.shtml

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 Hertfordshire Flowcharts for Managing an E-Safety 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 E-Safety Leader.
Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher.
Depending on the seriousness of the offence, sanctions could include 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

Flowcharts for Managing an E-Safety Incident

These three flowcharts have been developed by the HSCB E-Safety subgroup and are designed to help schools successfully manage E-Safety incidents http://www.thegrid.org.uk/eservices/safety/incident.shtml

Hertfordshire Flowchart to support decisions related to an illegal E-Safety Incident For Headteachers, Senior Leaders and E-Safety leaders

- Following an Incident the E-Safety Coordinator and/or Headteacher will need to decide quickly if the incident involved any illegal activity
- If you are not sure if the incident has any illegal aspects, contact for advice:
  - Herts E-Safety Adviser 01438 844893 – Kate Stockdale.
  - Youth Crime Reduction Officer.
  - Local Safe Neighbourhood Officer

- Illegal means something against the law such as:
  - Downloading child pornography
  - Passing onto others images or video containing child pornography
  - Inciting racial or religious hatred
  - Extreme cases of Cyberbullying
  - Promoting illegal acts
- Inform police and the Herts E-Safety Adviser (above). Follow any advice given by the police otherwise:
- Confiscate any laptop or other device and if related to 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 inform the Child Protection School Liaison Officer (CSPLO) on 01992 588182.
- If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 5556979

Was illegal material or activity found or suspected? If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents
Yes? No?
Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the E-Safety Leader.
If the incident did not involve and illegal activity then follow this flowchart:

Hertfordshire Managing an E-Safety Incident Flowchart for Headteachers, Senior Leaders and E-Safety Coordinators.

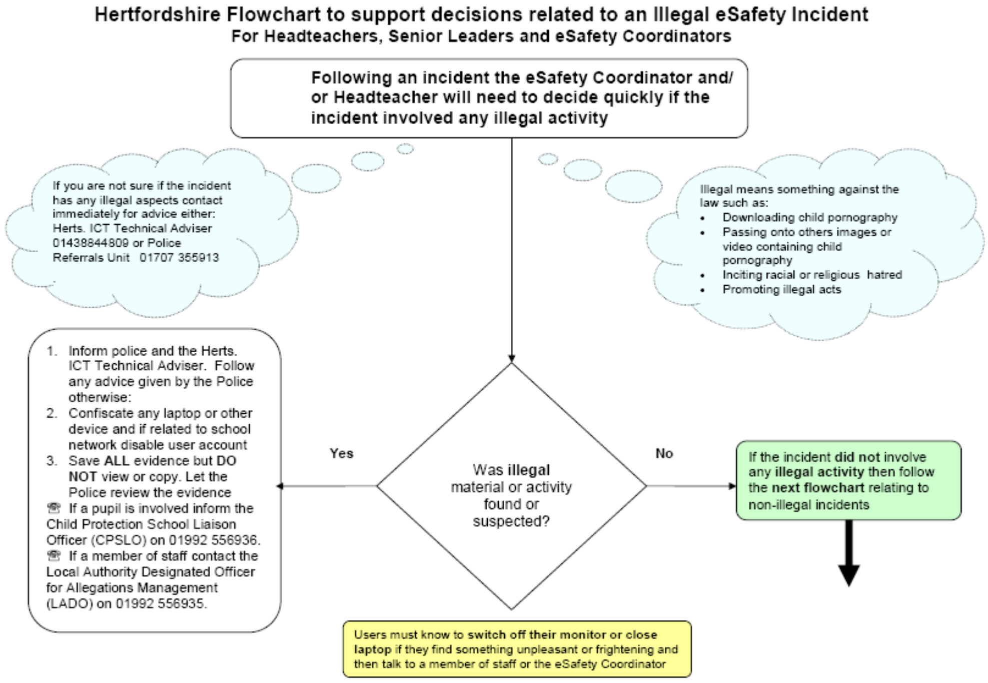
If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.
- Contact the LADO on: 01992 556979 If the incident does not satisfy the criteria in 10.1.1 of the HSCB procedures 2007, then follow the bullet points below:
- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact school HR, Rachel Hurst or
- Christopher Williams on 01438 844933

The E-Safety leader and/ or Headteacher should:

- Record in the school E-Safety Incident Log
- Keep any evidence

FLOWCHARTS FOR MANAGING AN ESAFETY INCIDENT



Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators

Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact immediately for advice either: Herts. ICT Technical Adviser 01438844809 or Police Referrals Unit 01707 355913

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Promoting illegal acts

Was **illegal** material or activity found or suspected?

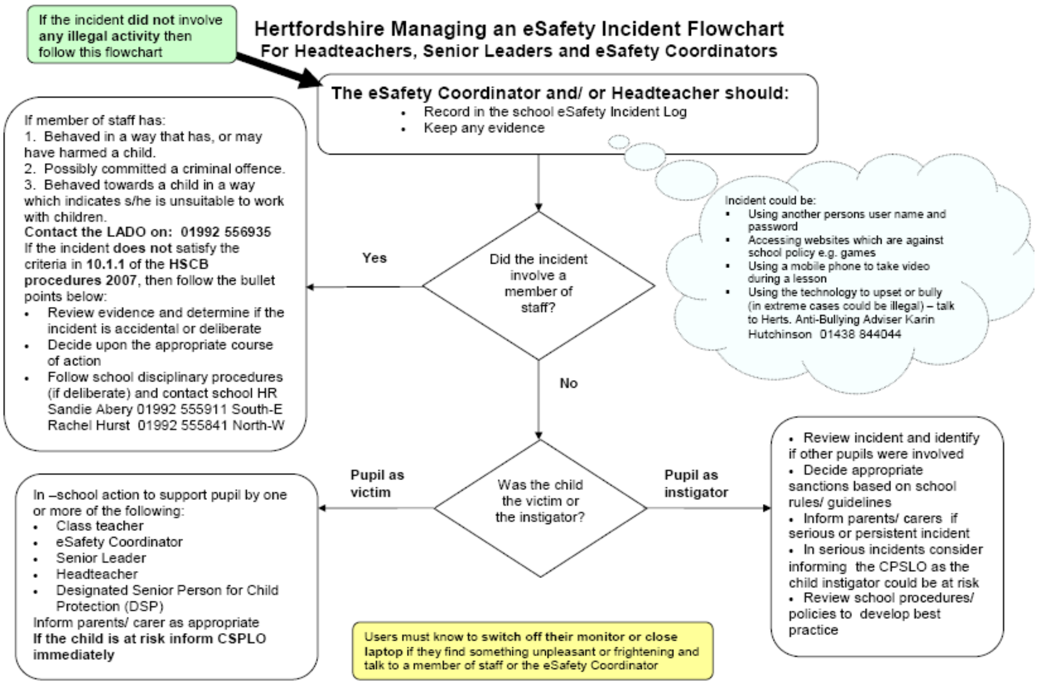
1. Inform police and the Herts. ICT Technical Adviser. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.

☎ If a member of staff contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 556935.

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



If the incident **did not** involve **any illegal activity** then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart
For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:

- Using another persons user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844044

Did the incident involve a member of staff?

If 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 which indicates s/he is unsuitable to work with children.

Contact the LADO on: 01992 556935
If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR Sandie Abery 01992 555911 South-E Rachel Hurst 01992 555841 North-W

Was the child the victim or the instigator?

In –school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader
- Headteacher
- Designated Senior Person for Child Protection (DSP)

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

Internet Access

The internet is an open worldwide communication medium, available to everyone, 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 internet use through the HICS network (Hertfordshire Internet Connectivity Service) 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 provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
Staff will preview any recommended sites, online services, software and apps before use.
Searching for images through open search engines is 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 the intended restricted audience.
Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
On-line gambling or gaming is not allowed.
It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/ filtered.shtml
- Our school also employs some additional web-filtering which is the responsibility of Lynsey Young and Andy Mari.
- Roebuck Primary School and Nursery 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 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 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 using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network managers to install or maintain virus

protection on personal systems. If pupils wish to bring in work on removable media it must be given to the (technician/teacher) for a safety check first.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Headteacher.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.
- Managing Other Online Technologies
- Online technologies, 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 endeavours to deny access to social networking and online games websites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such websites, 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 websites 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 websites 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 their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored

Parental 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 to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.
Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E-Safety policy through parent forums.
Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
The school disseminates information to parents relating to E-Safety where appropriate in the form of

- Information evenings
- Practical training sessions e.g. current E-Safety issues
- Posters
- School website information
- Newsletter items

Passwords and Password Security Passwords

- Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security
- http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata
- Always use your own personal passwords
- 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.
- 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.
- Never tell a child or colleague your password.
- If you aware of a breach of security with your password or account inform Headteacher immediately.
- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and or symbols.
- 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.
- Pupils are expected to keep their passwords private 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.

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, and remove any portable media from computers when not attended.
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.
- Please refer to the document on the grid for guidance on How to Encrypt Files

http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

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 another 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. HCC guidance can be found:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

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 pupils, staff and others without advance permission from the Headteacher.
Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

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
- on the school's learning platform or Virtual Learning Environment/ website
- 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 or carers may withdraw permission, in writing, at any time.
- Possible statements also be given in writing and will be kept on record by the school.

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

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see
http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

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 or other online school resource.
The Computing leader has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance
https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/
We do not use publicly accessible webcams in school.
Webcams will not be used for broadcast on the internet without prior parental consent.
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).
Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.
Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.
For further information relating to webcams and CCTV, please see
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtm

Video Conferencing

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.
- 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 to end-points beyond the 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.
- 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 and guidance relating to Video Conferencing, please see
http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

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

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- 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. You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. 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 device 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
- 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, mobile devices 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 the school 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. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. 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 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 and handed into the office in the morning. This technology may 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 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 iPads 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.
Never use a hand-held mobile phone whilst driving a vehicle.

Servers

Always keep servers in a locked and secure environment.
Limit access rights.
Always password protect and lock the server.
Existing servers should have security software installed appropriate to the machine's specification.
Backup tapes should be encrypted by appropriate software.
Data must be backed up regularly.
Backup tapes/discs must be securely stored in a fireproof container.
Back up media stored off-site must be secure.
Remote backups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777.

Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data. At the moment SITSS do not encrypt servers, however Office PCs (including Office Master PCs) installed by SITSS are supplied with encryption software installed.

Roebuck Primary School E-Safety rules

S afety. Don't put pictures of yourself or personal information on the computer. Do not talk to or believe strangers on line.

M essages sent to people we know must be kind.

A sk permission before using the internet, phones or playing with games.

R emember do not share your passwords. Report anything that makes you feel unsafe.

T hink and tell…
Think before you click and tell someone.

Review Procedure

There will be on-going opportunities for staff to discuss with the E-Safety coordinator any E-Safety issue that concerns them. There will be on-going opportunities for staff to discuss with the AIO any issue of data security that concerns them (state how, i.e. school council, staff meetings). This policy will be reviewed annually and consideration will be given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government changes the orders or guidance in any way.

The Governing Body reviews this policy every year. They governors may however, review the policy earlier than this, if the government introduces new regulations, or if the Governing Body receives recommendations on how the policy might be improved.

Date:
January 2018

Review Date:
January 2019