



'Valuing Potential; Creating Opportunities'

HARTSBOURNE PRIMARY SCHOOL

This policy to be read in conjunction with all other school policies

E-Safety and Data Security

Guidance Policies for ICT Acceptable Use

Release date: March 2015

Review date: March 2017

CONTENTS

| | | |
|---|----|-------------------------------------|
| RATIONALE..... | 1 | ERROR! BOOKMARK NOT DEFINED. |
| MONITORING..... | 2 | ERROR! BOOKMARK NOT DEFINED. |
| BREACHES | 3 | |
| Incident Reporting | 3 | |
| ACCEPTABLE USE AGREEMENT: PUPILS - PRIMARY | 4 | |
| ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS..... | 6 | |
| STAFF PROFESSIONAL RESPONSIBILITIES..... | 7 | |
| COMPUTER VIRUSES | 8 | |
| DATA SECURITY | 9 | |
| Security | 9 | |
| Protective Marking..... | 9 | |
| Relevant Responsible Persons..... | 10 | |
| Information Asset Owner (IAO)..... | 10 | |
| DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY | 11 | |
| E-MAIL..... | 12 | ERROR! BOOKMARK NOT DEFINED. |
| Managing e-mail..... | 12 | |
| Sending e-mails..... | 13 | |
| Receiving e-mails | 13 | |
| e-mailing Personal, Sensitive, Confidential or Classified Information | 13 | |
| EQUAL OPPORTUNITIES..... | 14 | |
| Pupils with Additional Needs..... | 14 | |
| ESAFETY..... | 15 | ERROR! BOOKMARK NOT DEFINED. |
| eSafety - Roles and Responsibilities..... | 15 | |
| eSafety in the Curriculum..... | 15 | |
| eSafety Skills Development for Staff..... | 15 | |
| Managing the School eSafety Messages | 15 | |
| INCIDENT REPORTING, ESAFETY INCIDENT LOG & INFRINGEMENTS | 16 | |
| Incident Reporting | 16 | |
| eSafety Incident Log..... | 16 | |
| Misuse and Infringements..... | 17 | |
| Flowcharts for Managing an eSafety Incident | 17 | |
| INTERNET ACCESS..... | 21 | |
| Managing the Internet..... | 21 | |
| Internet Use | 21 | |
| Infrastructure | 21 | |
| MANAGING OTHER ONLINE TECHNOLOGIES..... | 23 | |
| PARENTAL INVOLVEMENT..... | 24 | |
| PASSWORDS AND PASSWORD SECURITY | 25 | |

| | |
|---|----|
| Passwords..... | 25 |
| Password Security..... | 25 |
| Zombie Accounts..... | 26 |
| PERSONAL OR SENSITIVE INFORMATION..... | 27 |
| Protecting Personal, Sensitive, Confidential and Classified Information..... | 27 |
| Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media..... | 27 |
| REMOTE ACCESS..... | 28 |
| SAFE USE OF IMAGES..... | 29 |
| Taking of Images and Film..... | 29 |
| Consent of Adults Who Work at the School..... | 29 |
| Publishing Pupil's Images and Work..... | 29 |
| Storage of Images..... | 30 |
| Webcams and CCTV..... | 30 |
| Video Conferencing..... | 30 |
| ICT EQUIPMENT INCLUDING PORTABLE/MOBILE EQUIPMENT, REMOVABLE MEDIA..... | 32 |
| School ICT Equipment..... | 32 |
| Portable & Mobile ICT Equipment..... | 32 |
| Mobile Technologies..... | 33 |
| TELEPHONE SERVICES..... | 34 |
| Removable Media..... | 35 |
| SERVICES..... | 35 |
| SMILE AND STAY SAFE POSTER..... | 36 |
| SOCIAL MEDIA, INCLUDING FACEBOOK AND TWITTER..... | 37 |
| SYSTEMS AND ACCESS..... | 38 |
| WRITING AND REVIEWING THIS POLICY..... | 39 |
| Staff and Pupil Involvement in Policy Creation..... | 39 |
| Review Procedure..... | 39 |
| FURTHER HELP AND SUPPORT..... | 40 |
| CURRENT LEGISLATION..... | 41 |
| Acts Relating to Monitoring of Staff email..... | 41 |
| Other Acts Relating to eSafety..... | 41 |
| Acts Relating to the Protection of Personal Data..... | 43 |
| APPENDIX..... | 44 |
| Information Risk Actions Form..... | 44 |
| School Policy in Brief..... | 45 |

RATIONALE

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/watches with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs, Wikis, Podcasting
- Video sharing
- Downloading/uploading, video sharing
- '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 Hartsbourne 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 others 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 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, smart watches 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.

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.

Consequences for pupils who breach our ICT and data protection policies will be in line with our 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 SecureID 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: **The Head Teacher, Deputy Head Teacher, School Business Manager.**

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use Agreement / eSafety Rules

I AGREE THAT I WILL:

- Only use ICT in school for school purposes.
- Only use my class e-mail address or my own school e-mail address when e-mailing.
- Only open e-mail attachments from people I know, or who my teacher has approved.
- Keep my passwords private from other people.
- I will only open/delete my own files.
- Not use a memory stick or flash drive to transfer files from home to school.
- Make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- Tell my teacher if I accidentally find anything unpleasant or nasty and I will not deliberately look for, save or send anything that could be considered inappropriate.
- Not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image.
- Be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- Support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- Agree that my use of ICT is checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.

Signed:

Date: March 2016

Sample letter for admission packs:

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Head Teacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.



Parent/ carer signature

We have discussed this document with(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Hartsbourne Primary School.

Parent/ Carer Signature

Class Date



Acceptable Use Agreement: Staff, Governors and Visitors

HARTSBOURNE PRIMARY SCHOOL 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 the Head Teacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable 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, personal Twitter account, or any other social media link, 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 in school and will not be taken off school premises.
- Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- All personal data and images of pupils will be uploaded to the T drive of the school server and not saved to a desktop or local hard drive.
- Personal memory sticks will not be used to upload documents to school computers or our local server.
- Staff may e-mail documents and images to school and save to the appropriate intranet drive.
- I will not install any hardware or software without permission of the Head Teacher.
- 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 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 Head Teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- 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 Head teacher
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- 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.

User Signature

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

SIGNATURE FULL NAME:
JOB TITLE DATE:

Staff Professional Responsibilities

The HSCB eSafety 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>



PROFESSIONAL RESPONSIBILITIES **When using any form of ICT, including the Internet,** **in school and outside school**



For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.



- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.



- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.



- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.



- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.



- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.

- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893



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 (see previous items regarding memory sticks).
- 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 immediately and contact your ICT support provider as soon as possible. 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 taken very seriously at Hartsbourne. Local Authority guidance documents are 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

- 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 all passwords secure and change regularly.
- Staff are made aware of their responsibility when accessing school data and have been made aware of the relevant guidance and the Policy for Acceptable Use.
- Appropriate 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>)
- Staff must not leave any portable or mobile ICT equipment or removable storage media in unattended vehicles; it should be kept with the staff member 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.
- Anyone sending a confidential or sensitive e-mail should use the designated confidential websites from Herts County Council.

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 types 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. The School Business Manager has the following responsibilities:

- Lead on the information risk policy and risk assessment
- Advise school staff on appropriate use of school technology
- 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. The School Business Manager should identify:

- 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 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

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

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 (eg 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

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

The Waste Electrical and Electronic Equipment Regulations 2006

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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

Information Commissioner website <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. Please note the following conditions:

- 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: '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. All children will use a class/ group e-mail address only (no individual accounts).
-
- E-mails created or received as part of a school role 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 archive.

The forwarding of chain emails is not permitted in school. However the school will consider using a dummy address to allow pupils to forward any chain emails causing them anxiety. No action will be taken with this account by any member of the school community.

All pupil 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.

Please note:

- Encourage pupils to tell a trusted adult if they receive an offensive or upsetting e-mail.
- Staff must inform the Head or Deputy Head if they receive an offensive e-mail.
- However you access your school e-mail; 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 use the secure Hertfordshire webmail facility.
- 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 of any kind.

Receiving e-mails

- Staff should check e-mail regularly and consider activating an '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 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' eSafety 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 eSafety issues.

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

E-SAFETY

Roles and Responsibilities

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 the Head Teacher who has been designated this role as a member of the senior leadership team and DSP. 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 Herts LA, Herts for Learning Ltd, 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 PSHCE.

eSafety in the Curriculum

The school follows the Herts for Learning Ltd Computing and ICT curriculum (available from the school intranet) which is a comprehensive framework for teaching a variety of computing skills including e-safety.

We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis rather than an 'event' or one-off lesson. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

Pupils are made aware of the impact of Cyber-bullying and are taught to seek help if any form of online bullying affects them. Pupils are also made 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.

eSafety Skills Development for Staff

Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of staff meetings, staff briefings, inset and CPD opportunities. 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 eSafety and know how to report the misuse of technology by any member of the school community to the Head Teacher.

Managing the School eSafety Messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used. The key eSafety advice will be promoted widely through school displays, newsletters, class activities and participation in events such as Safer Internet Day.

INCIDENT REPORTING, INCIDENT LOG AND 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 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 Information Asset Owner.

eSafety Incident Log

Details of e safety incidents will be recorded by the Head Teacher and monitored by the SLT and Governors. Incidents of cyber bullying will be recorded in the Behaviour Record file, kept by the Head Teacher. Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

| Date & Time | Name of pupil or staff member | Male or Female | Room and computer/ device number | Details of incident (including evidence) | Actions and reasons |
|-------------|-------------------------------|----------------|----------------------------------|--|---------------------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

This can be downloaded <http://www.thegrid.org.uk/eservices/safety/incident.shtml>

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 **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material

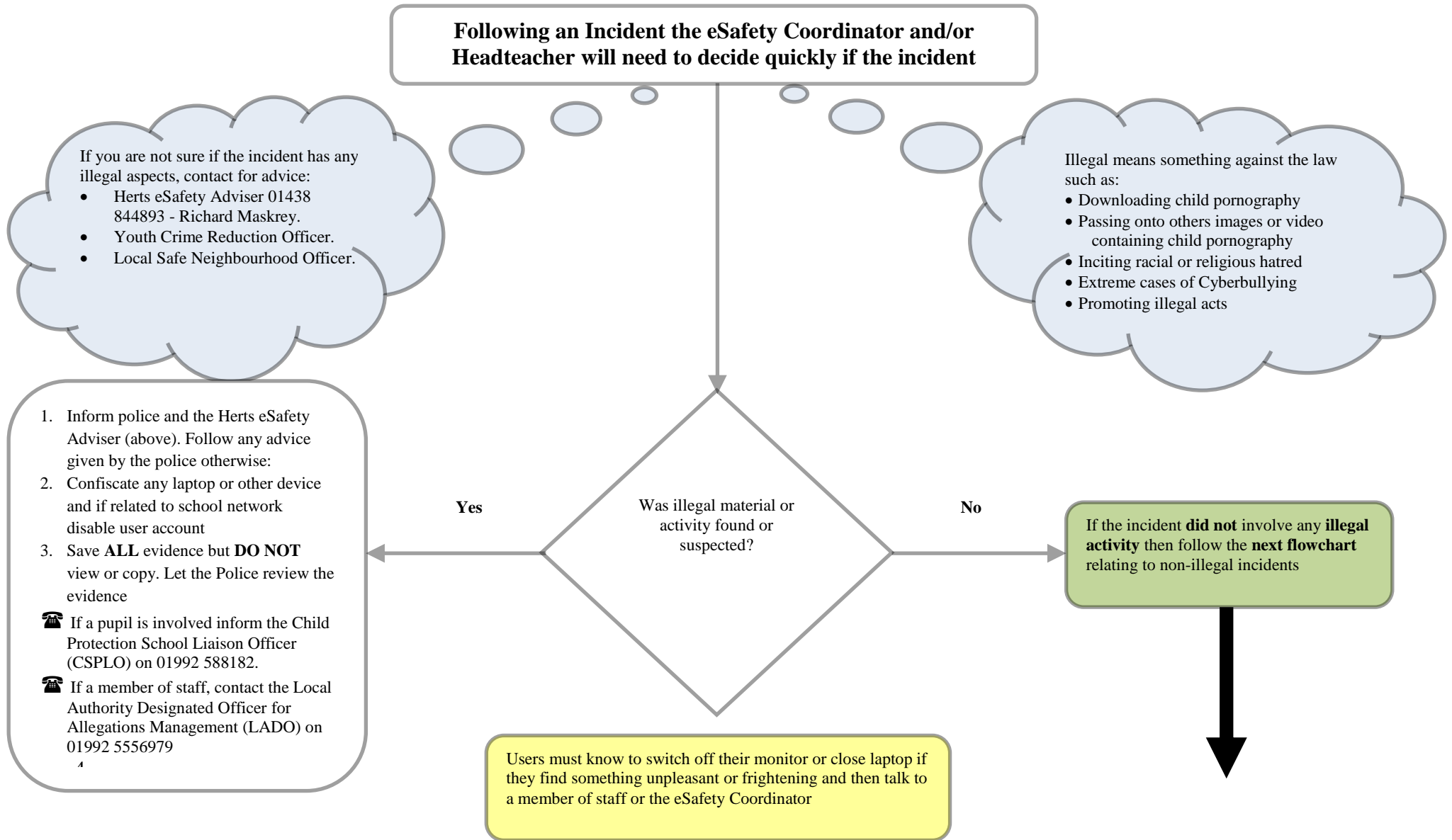
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher and or Governors as appropriate. 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 by this policy and staff handbook.

Flowcharts for Managing an eSafety Incident

These three flowcharts have been developed by the HSCB eSafety subgroup and are designed to help schools successfully manage eSafety incidents

<http://www.thegrid.org.uk/eservices/safety/incident.shtml>

Hertfordshire Flowchart to support decisions related to an illegal eSafety Incident For Head Teachers, Senior Leaders and eSafety Coordinators



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

Hertfordshire Managing an eSafety Incident Flowchart For Head Teachers, Senior Leaders and eSafety 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

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

- Class teacher
 - eSafety Coordinator
 - Senior Leader or Headteacher
 - Designated Senior Person for Child Protection (DSP)
 - School PCSO
- Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.

The eSafety Coordinator and/ or Headteacher should:

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

Did the incident involve a member of staff?

Yes

No

Was the child the victim or the instigator?

Pupil as victim

Pupil as instigator

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

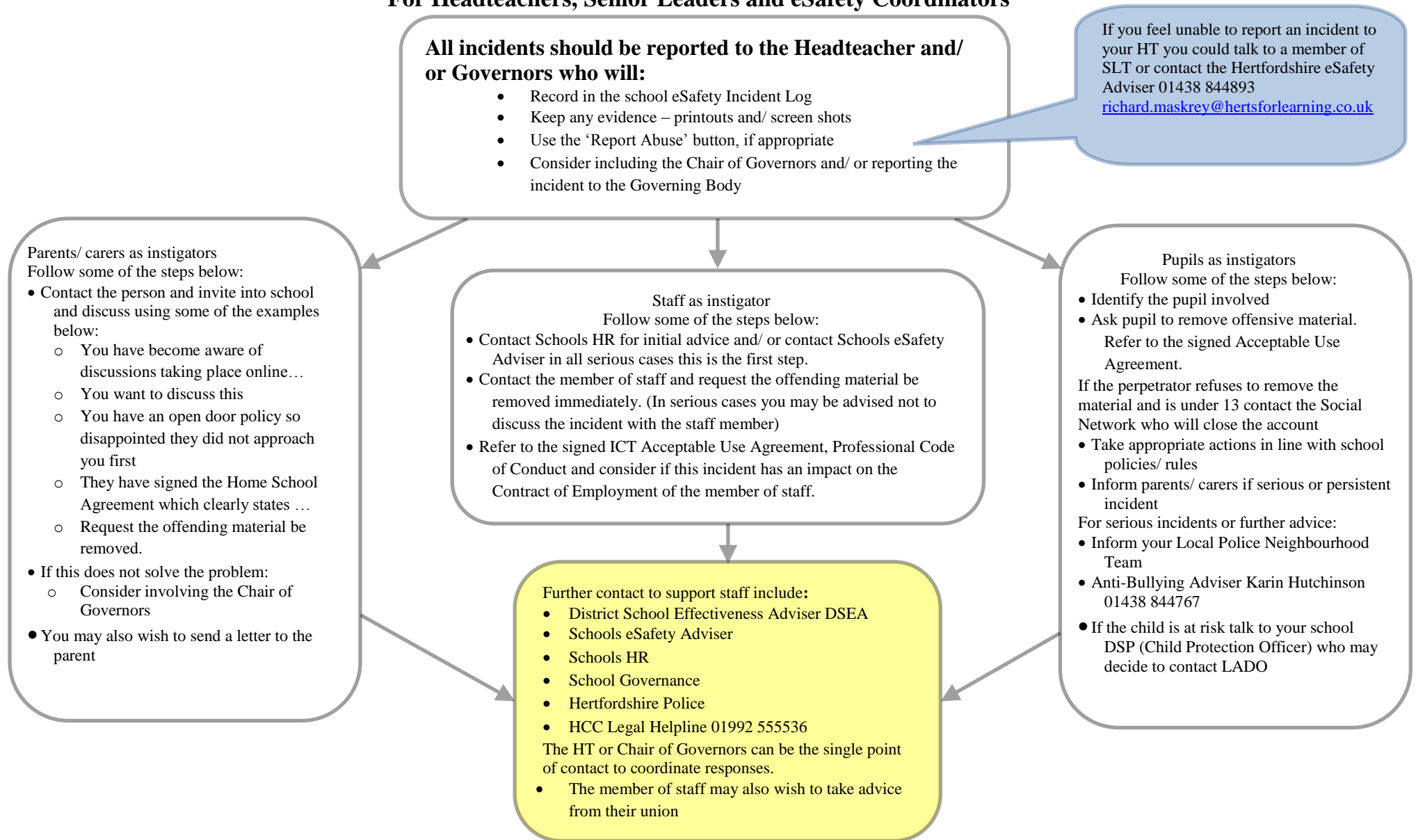
Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- 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 84476

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support 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

Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and eSafety Coordinators



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

- Staff 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 on school premises or using school equipment off site.

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>

- Hartsbourne Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and 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.
- 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 School Business 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 from the Head teacher.
- If there are any issues related to viruses or anti-virus software, the Head and/or School Business Manager should be informed in person as soon as possible.

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.

- Currently the school endeavors to deny access to social networking and online games websites to pupils within school.
- 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)
- 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 Head Teacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored <http://www.coppa.org/comply.htm>.

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 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 of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through parent and pupil questionnaires, school Council Meetings, Parents' Forum meetings.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- 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 (eg, on school website, in displays).
- Parents/carers are expected to sign a Home School agreement containing the following statement
 - We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.
- The school disseminates information to parents relating to eSafety where appropriate through weekly newsletters, school website information, displays and posters in school, Parents' Forum meetings.

PASSWORDS AND PASSWORD SECURITY

Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which also contains guidance on creating strong passwords and password security.

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

- Always use your own 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.
- Never tell a child or colleague your password.
- If you are aware of a breach of security with your password or account inform the Head or SLT member immediately.
- Passwords must contain a minimum of six characters and be difficult to guess. They should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within TWO WEEKS.

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 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.
- Pupils are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff

users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is **five minutes**.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).
- In our school, all ICT password policies are the responsibility of the ICT support Assistant and/or School Business Manager 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 unauthorised access

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 Copiers (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.

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, eg 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. HCC guidance can be found:

<http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse>

Possible statements

- 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 website, in the school prospectus and other printed publications, recorded by video or webcam, display materials in communal areas and external areas (eg an exhibition), general experiences that may be sent to local and/or national press (traditionally or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in circumstances where consent is withdrawn (eg a custody issue).

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

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 Head, Deputy, School Business Manager, ICT Support Assistant, has authority to upload to the internet.

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 and a removable hard drive kept by the Head Teacher.
 - Pupils and staff are not permitted to use personal portable media for storage of images.
 - 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.
 - Class teachers must delete the images when they are no longer required, or when the pupil has left the school.
-

Webcams and CCTV

- 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).
 - Webcams can be found on class and teacher i-pads, laptops, flip devices for curriculum use only.
 - 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 devices.

For further information relating to webcams and CCTV, please see

<http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml>

Video Conferencing

- Permission is sought from parents/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 Head teacher is sought prior to all video conferences within school to end-points beyond the school.
- The school conferencing equipment 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 DBS (previously 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 and guidance relating to Video Conferencing, please see

<http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml>

SCHOOL EQUIPMENT INCLUDING PORTABLE AND MOBILE ICT AND REMOVABLE MEDIA

School ICT Equipment

- All users of school ICT equipment are responsible for their own activities.
- The school logs ICT equipment issued to staff and records serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- 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 as 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 who are walking home alone are allowed to bring a mobile phone to school which must be left in the school office and collected at the end of the day. The device must be clearly named and switched onto silent for the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- 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 members 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.

Telephone Services (Landlines)

- 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 HCC 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.
 - Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures are available through the Emergency Response Plan.
-

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.

Smile and Stay Safe Poster



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.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment during school hours.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

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.
- Ensure you remove portable media from your computer when it is left unattended.
- 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 HCC 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 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 the data.

Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through school council meetings, staff meetings, INSET, Parents' Forum meetings).

Review Procedure

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety 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.

This policy will be reviewed every (24) months 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 change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors in March 2016.

Further help and support

Your organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998. For more information visit the website of the Information Commissioner's Office <https://ico.org.uk/>

Advice on eSafety - <http://www.thegrid.org.uk/eservices/safety/index.shtml>

Further guidance - <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

School's toolkit is available - Record Management Society website – <http://www.rms-gb.org.uk/resources/848>

Test your online safety skills <http://www.getsafeonline.org>

Data Protection Team – email - data.protection@hertfordshire.gov.uk

Information Commissioner's Office – www.ico.org.uk

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2014. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based “cloud” service provision – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

For additional help, email school.ictsupport@education.gsi.gov.uk

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

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

<http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

<http://www.hmsso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “*Children & Families: Safer from Sexual Crime*” document as part of their child protection packs.

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3) Regardless of an individual's motivation, the Act makes it a criminal offence to gain access to computer files or software without permission (for example using another person's password to access files), to gain unauthorised access to commit a further criminal act (such as fraud) and/or impair the operation of a computer programme.

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 their 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 2000

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

Appendix 2

Hartsbourne Primary School Policy in Brief

At this school:

- We have an Acceptable Use policy which is reviewed at least annually, which all staff sign. Copies are kept on file and we use the LA model policy and model agreements.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.
- Protected and restricted material must not be removed from the school.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We follow LA guidelines for the transfer of any other internal data.
- Sensitive or personal material on paper is held in a lockable storage cabinet.
- All servers are in lockable locations and managed by CRB-checked staff.
- At this school we follow Hertfordshire local authority back-up procedures.
- We use SITTS protocols for disaster recovery on our admin server.
- Staff do not use memory sticks or flash drives to transfer information or files.
- Staff do not use personal mobile devices for contacting pupils or parents or taking videos or photographs.
- Staff must upload images and other sensitive information to the school server as soon as practicable (do not store on desktops or local hard drives).

Passwords

- Always use your own passwords and enter each time you logon (do not save passwords in any automated logon procedures).
- Change temporary passwords at first logon and whenever there is an indication of password compromise. Inform the Head or SLT immediately you suspect a breach of security.
- 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 (including pupils and colleagues). 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. They should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within TWO WEEKS.

Disposal of files:

- Sensitive or personal material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.
- We use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- Paper based sensitive information is shredded.
- School laptops used by staff are disposed of through the same procedure.
- From 2009 all laptops have been set-up with laptop hard drive encryption.

Staff with access to setting-up usernames and passwords which enable users to access data systems eg for email, network access, SLG and Learning Platform access report to the Head Teacher and School Business Manager.

Security policies are reviewed and staff updated at least annually. Staff know to report any incidents where data protection may have been compromised. Staff have been issued with guidance documentation.

© Herts for Learning 2015

Copyright of this publication and copyright of individual documents and media within this publication remains with the original publishers and is intended only for use in schools.

All rights reserved. Extracts of the materials contained on this publication may be used and reproduced for educational purposes only. Any other use requires the permission of the relevant copyright holder.

Requests for permissions, with a statement of the purpose and extent, should be addressed to Herts for Learning Ltd, SROB210, Robertson House, Six Hills Way, Stevenage, SG1 2FQ or telephone 01438 844893.