



Ss Alban & Stephen Infant & Nursery School

eSafety

and

Data Security

Policies for ICT Acceptable Use

(Based On Herts for Learning Model policies)

Version date: March 2016

Review date: March 2018

CONTENTS

Introduction	1
Monitoring, Breaches, Incident reporting, Computer viruses	2
Data Security, disposal of equipment	3
Email – managing, sending & receiving, emailing personal or confidential information..	4
e-Safety – roles & responsibilities, curriculum, pupils with additional needs.....	5
- Skills development for staff, school safety message, incident log.....	6
- Misuse & infringements, managing an incident.....	7
- Flowcharts for incident management.....	8-10
Internet access, managing the internet, internet use, Infrastructure	11
Parental involvement	12
Passwords, password security	13
Zombie accounts, protecting & storing sensitive information, remote access.....	14 – 15
Safe use of images – taking, storing & publishing work & images, consent	16 – 17
School ICT equipment – portable & mobile	18
Mobile devices – personal, school provided, removable data.....	18.–19
Removable media, servers	20
Social Media, including Facebook & Twitter	20
Staff & Pupil involvement in policy, Review procedure	21
Further help & support	22
Current legislation.....	23 – 25
Appendix 1 - School policy in Brief	26
Pupil acceptable use agreement	27
Parent form to accompany pupil acceptable use agreement	28
Staff, governor & visitor acceptable use agreement & code of conduct	29
Staff professional responsibilities	30

INTRODUCTION

At **Ss Alban & Stephen Infants 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.

The purpose of this policy is to:

- Make all users aware of the range of risks associated with the use of internet technologies & that many have minimum age requirements (mostly 13 years)
- Remind everybody in the school community of our shared responsibility to secure any sensitive information used in their day to day professional duties

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors 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).

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, equipping 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, constantly changing and evolving. Currently the internet technologies children and young people may be using both inside and outside of the classroom include:

- Websites
- Apps
- Email, 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

- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Monitoring

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.

Incident Reporting

Any security breaches, loss of equipment, virus notifications, unsolicited emails, or suspected misuse of ICT must be immediately reported to the school's relevant responsible person, **Bernadette Dempsey, Head teacher.**

Computer viruses

- All files downloaded from the Internet, received via email 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 you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact our ICT technician or the Head teacher immediately.
-

Data Security

Data Protection: key responsibilities for School Heads and Governors

The accessing and appropriate use of school data is taken very seriously. HCC guidance documents can be found at:

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

Security

- The school gives relevant staff access to its Management Information System, SIMS 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 keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- When out of school, 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. Portable equipment should be securely stored when not in use or unattended (e.g. evenings, weekends, holidays).
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed.

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 overwritten multiple times to ensure the data is irretrievably destroyed or physically destroyed. Disposal of any ICT equipment will conform to:

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
 - How it was disposed of e.g. waste, gift, sale
 - Name of person & / or organisation who received the disposed item
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

<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

email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- Staff & governors should use their school email for all professional communication. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Staff should not contact pupils, parents or conduct any school business using personal email addresses
- The school requires a standard disclaimer to be attached to all email 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
- Emails 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.
- Pupils are introduced to email as part of the Computing Programme of Study & use a class/ group email address

- Staff must inform (the Head teacher or line manager) if they receive an offensive email
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information
- Use your own school email account so that you are clearly identified as the originator of a message
- School email is not to be used for personal advertising

Receiving emails

- Check your email regularly
- Never open attachments from an untrusted source; consult the ICT technician first

Emailing Personal or Confidential Information

- Where your conclusion is that email must be used to transmit such data:

Either:

Use Schoolsfx, Hertsfx or 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>

Or:

Obtain express consent from your manager to provide the information by email and exercise caution when sending the email and always follow these checks before releasing the email:

- Encrypt and password protect. See <http://www.thegrid.org.uk/info/dataprotection/#securedata>
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email 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 email
 - 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 email
 - Request confirmation of safe receipt
-

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is **Bernadette Dempsey** who has been designated this role **as Head teacher**. 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 HCC, 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

eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school provides opportunities within a range of curriculum areas to teach about eSafety. Internet skills and safety are explicitly taught in weekly Computing & ICT lessons. Pupils are educated on online risks that they may encounter outside school both informally when opportunities arise and as part of eSafety in the Herts Computing curriculum
- 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 Childline or the 'CEOP report abuse' button
-

Pupils with Additional Needs

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 are planned and well managed for these children and young people.

eSafety Skills Development for Staff

- 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 what to do in the event of misuse of technology by any member of the school community (see eSafety Coordinator)
-

Managing the School eSafety Messages

- The eSafety policy will be introduced to the pupils at the start of each school year
 - eSafety posters will be prominently displayed
 - The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on
 - Pupils, staff, parents & governors will be offered eSafety training (as offered in workshops with Richard Maskrey in November 2015) We will participate in Safer Internet Day every February.
-

eSafety Incident Log

An incident log will be kept by the Designated Person responsible for esafety, **Bernadette Dempsey** & reported to governors.

'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

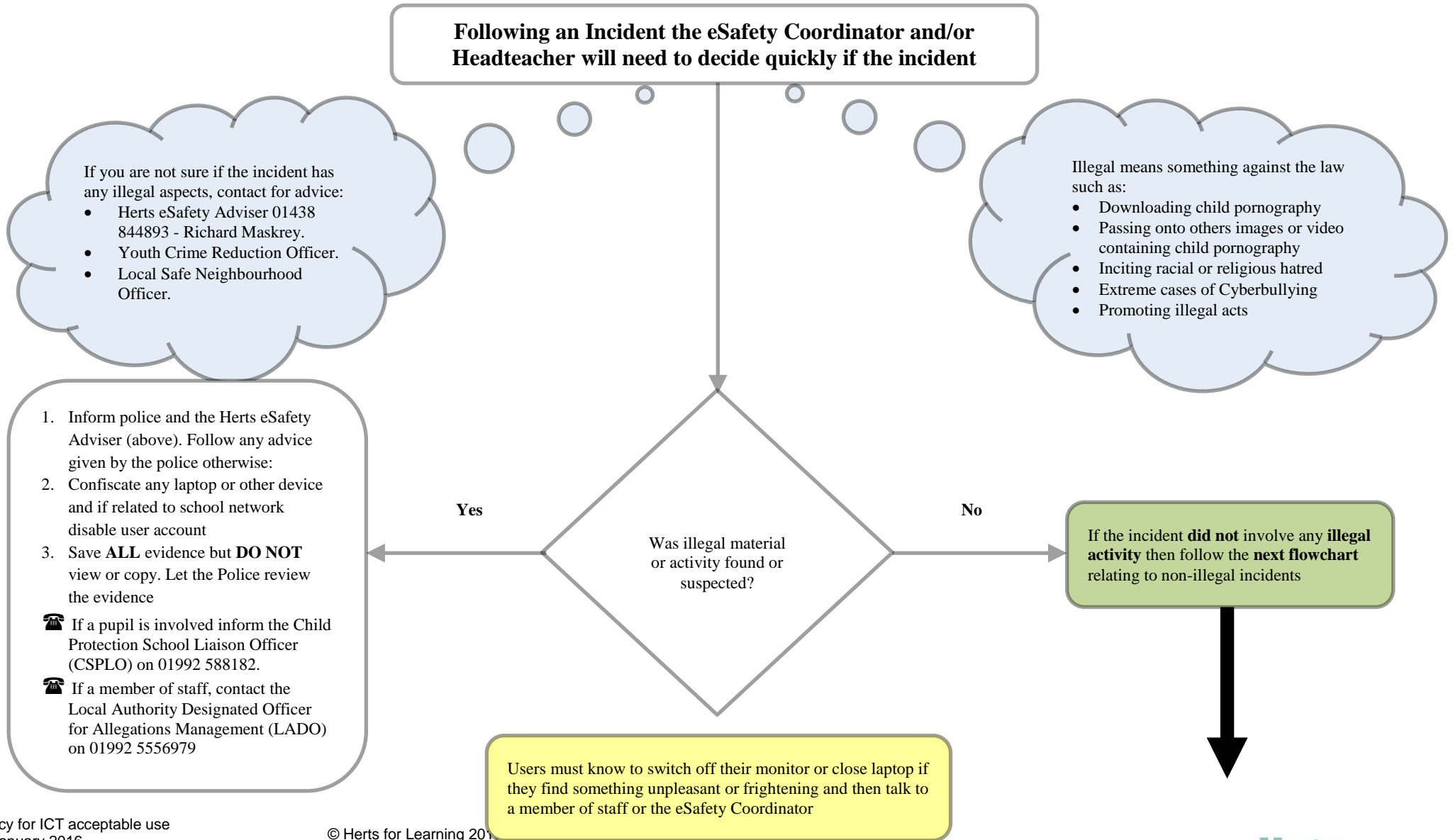
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person,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

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 Headteachers, 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 Headteachers, 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 at HfL on 01438 845111

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

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 at HfL on 01438 845111

Was the child the victim or the instigator?

Pupil as victim

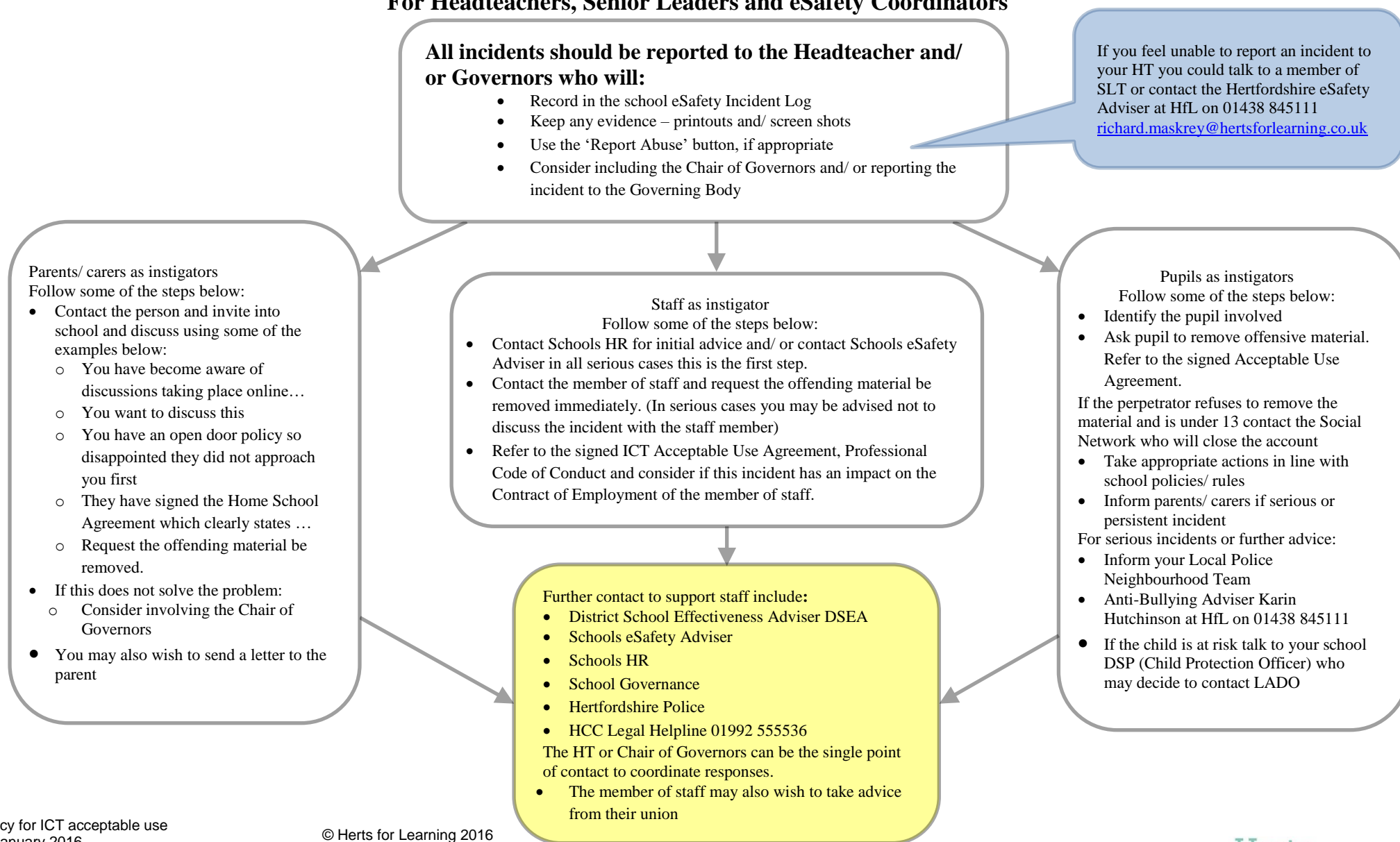
Pupil as instigator

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

- 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 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
 - Parents will be advised to supervise any internet research for homework
 - 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

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

Infrastructure

- Schools subscribing to the HICS web filtering service have the benefit of monitored web activity. For further information relating to filtering please go to <http://www.thegrid.org.uk/eservices/safety/filtered.shtml>
- **Ss Alban & Stephen Infants 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)

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 by giving feedback on policy documents and training/information provided by school.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child when these are updated
- 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)
- Parents/carers are expected to sign a Home School agreement containing the following statement(s)
 - **I/we will support the school approach to online safety and not 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.**
 - **I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information evenings
 - Practical training sessions e.g. current eSafety issues
 - Posters
 - School website information
 - Newsletter items

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
- **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 the Head teacher immediately**

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.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security

- Users are provided with an individual network, email, learning platform and/or Management Information System log-in username. From **01/04/16** they are also expected to use a personal password and keep it private
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the school learning platform on shared or private computers

Zombie Accounts

Zombie accounts refers to accounts belonging to all users who have left the school and therefore no longer have authorised access to the school's systems. The school secretary will disable such accounts within 1 week, once the member of the school staff has left.

Protecting Personal or Sensitive 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 that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print to shared copiers/printers 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 or sensitive 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 or Sensitive Information Using Removable Media

- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Use Schoolsfx for data transfers or encrypt all files containing personal or sensitive data

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

- Remote access is provided to a limited number of school staff and at the discretion of the Head Teacher. 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
- 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 here: <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

- 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 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
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school

Model policy for ICT acceptable use
Issue 10 January 2016
© Herts for Learning 2016

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. 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. Email 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 those staff designated by **Website Manager, Debbie Doherty or the Head teacher, Bernadette Dempsey** have 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 in Website history
- 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
- **Website Manager, Debbie Doherty** has the responsibility of deleting the images when they are no longer required.

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- School maintains a log of ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Ensure that all ICT equipment that you use is kept physically secure
- 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
- 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 Head teacher or 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.
- 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

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. School does not allow a member of staff to contact a pupil or parent/ carer using their personal device
- Year 6 Pupils attending Breakfast club are allowed to bring personal mobile devices/phones to school but must surrender them to staff on arrival at school.
- Parent helpers are asked to give mobile phones to office staff for safe keeping on arrival at school, to be returned when parents leave. Visitors are asked to switch mobile phones off/ put on silent and refrain from using them throughout their time in school.
- 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

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal or Sensitive Information Using Removable Media**'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- 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
- 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

Social Media, including Facebook and Twitter

- Staff **are not** permitted to access their personal social media accounts using school equipment during school hours
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- 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

should at all times be compatible with UK law

Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through assemblies, ICT lessons, school council, staff and governor meetings
-

Review Procedure

There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue 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 on **...11 May 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 2015. 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/publications/cloud-software-services-and-the-data-protection-act>

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

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

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

Regulation of Investigatory Powers Act 2000

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

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

Human Rights Act 1998

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

Other Acts Relating to 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)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) 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/>

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

<https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services>

Appendix 1

School Policy in Brief – Ss Alban & Stephen Infants School

- At this school we have an Acceptable Use policy which will be reviewed annually & which all staff sign. Copies are kept on file. We use the LA model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students. We use the LA model agreements.

Personal or sensitive material must not be removed from school.

- At this school we use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer

Personal or sensitive material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in lockable storage cabinets in the school office or Head teacher's office.
- At this school we use follow LA back-up procedures.

Disposal: personal or sensitive material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, etc, are controlled by School secretary, supported by the LA ICT Support Service and our school ICT technician.
- Security policies are reviewed and staff updated at least annually. Staff should report any incidents where data protection may have been compromised to the Head Teacher.



Ss Alban & Stephen Infant School & Nursery

Acceptable Use Agreement / eSafety Rules

For pupils

- If I see something I don't like, or something pops up on my screen, I will tell an adult I can trust
- I will keep any passwords private and not share them with my friends
- I will be nice to people online and treat them like I would in the playground or classroom
- People playing games are strangers so I will not share personal information or photos of myself

For parents

- I will support the school approach to online safety
- I will ensure that my activity online or on social media is not offensive or disrespectful to other members of the school community

Dear Parent/ Carer

ICT including the internet, email 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 Mrs Dempsey.

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 Ss Alban & Stephen Infants School.

Parent/ Carer Signature

Class Date

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as 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 **Bernadette Dempsey, Head Teacher**.

- I will only use the school's email / Internet / Intranet 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 email address, personal Twitter account, or any other social media link, 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 MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher
- 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 Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its 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 Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, 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 will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.45am and 3.15pm, except in the staff room and where there are signs to indicate this. I will keep these items in a school locker unless I have made specific arrangements with the Head teacher or Senior Leadership Team (in very exceptional circumstances)
- 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 Date

Full Name (printed)

Job title

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



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. © Herts for Learning 2016