Hertfordshire County Council

Children, Schools and Families

Goldfield Infants' and Nursery School

eSafety and Data Security Policy

Committee	Learning Matters
Next Review	Autumn 2017
Duration	1 year
Approved FGB	Autumn 2016
Reviewed	Spring 2018 Awaiting new County Model

Hertfordshire

Guidance

Once this policy has been ratified by the School's Governors it will be issued to all personnel, including Governors and pupils, involved in the working of the school.

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

Goldfield will ensure that all persons, including Governors, who join the establishment mid-year are provided with the policy and agreement.

Introduction

Goldfield Infants' and Nursery School recognises that ICT is now an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of our children and the wider community. Consequently, we aim to equip our pupils with the skills needed to access safely the range of technologies available and to use them in 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 and Apps
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading, including On Demand TV and video, movies, radio and Smart TV
- Online games
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality, including tablets and gaming devices

Whilst we recognise the exciting and beneficial aspect of these technologies, both in and out of the context of education, we also appreciate the potential dangers. All users need to be made aware of the range of risks associated with the use of these Internet technologies.

At Goldfield 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.

All schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. Consequently everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised HCC staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any breach of this policy is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the HCC Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;

- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SRP (Senior Responsible Person) who is the Head teacher and Designated Person for Safeguarding, or to the eSafety Co-ordinator, who is the Deputy Designated Person for Safeguarding. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secured tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SRP or eSafety Coordinator.

Computer Viruses

• All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB pens, CD) must be checked for any viruses using school provided anti-virus software before using them

•Never interfere with any anti-virus software installed on school ICT equipment that you use

•If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

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

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Detailed guidance on this can be found in the following documents

- HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Head teacher'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

- SRP Guidance – Data Security in Schools - Dos and Don'ts

The Head, SRP and Network Manager documents contain advice about identifying information assets including an example of an excel spreadsheet and a brief outline of the school policy that can be displayed at appropriate sites within the school or handed to visitors or guests.

•The School gives relevant staff access to its Management Information System, with a unique ID and password

•It is the responsibility of everyone to keep passwords secure

•Staff are aware of their responsibility when accessing school data

•Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

•Staff have access, and it is their responsibility to 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/traded/sitss/)

•Leadership have identified a Relevant Responsible Person (SRP) as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)

•Staff keep all school related data secure. This includes all personal, or confidential data

•Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

•Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

•It is the responsibility of individual staff to ensure the security of any personal or confidential information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax should have warned the sender to notify before it is sent.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. Previously called a Senior Information Risk Officer (SRP), there should be a member of the senior leadership team who has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

:

- they own the information risk policy and risk assessment

- • they act as an advocate for information risk management

The Office of Public Sector Information has produced Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SRPs in their role.

The SRP in this school is Debbie Stevens, Head teacher.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency or via the Hertfordshire Business Services (HBS) disposal scheme. 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

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

- The school's disposal record will include:

    - Date item disposed of

    - Authorisation for disposal, including:

        - verification of software licensing

        - Any personal data likely to be held on the storage media*

    - How it was disposed of e.g. waste, gift, sale

    - Name of person & / or organisation who received the disposed item

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

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

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

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

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/computers/pc_disposal.shtml

e-Mail

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. Educationally, email 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 email in relation to their age and how to behave responsible online.

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 e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils or parents to conduct any school business using personal e-mail addresses

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, ‘the views expressed are not necessarily those of the school or the LA’. This disclaimer has been added to each school account. The responsibility for maintaining this disclaimer lies with the account holder

- All e-mails should be written and checked before sending, with the same care as a letter written on school headed paper, as it represents the school.

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or admin account

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value

- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- Staff must inform the eSafety coordinators (DS or AN) if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT Scheme of Work

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving confidential school information is not permitted. Please refer to the Section **Error! Reference source not found.**

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section specific to this topic.

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

- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

- School e-mail is not to be used for personal advertising Receiving e-Mails

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

- Never open attachments from an untrusted source; Consult your network manager first.

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

- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal or confidential Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

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

  - Obtain express consent from your manager to provide the information by e-mail

  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information

    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information

    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)

  - Send the information as an encrypted document **attached** to an e-mail

  - Provide the encryption key or password by a **separate** contact with the recipient(s)

  - Do not identify such information in the subject line of any e-mail

  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Hertfordshire Constabulary

– Hertfordshire Partnership Trust

Future Developments

There is currently a review taking place on the way e-mails are sent whereby all such communications are sent using GCSx.

GCSx stands for the Government Connect Secure eXtranet. It provides a more secure communications system (i.e. more secure than the internet).

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy etc.). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

We at Goldfield recognise that not all parents or children may have equal access to the internet or to the use of various technologies at home. All email communication with parents is also available in hard copy. Every effort is made to sensitively identify those parents/carers who require or prefer this. All parents are invited to ask for access to the internet if they cannot access it at home.

Pupils with Additional Needs

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

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

Due to the young age of our children careful consideration is given to pupils when raising awareness of eSafety. Internet activities are planned and well managed for these children.

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 Leader in this school is the Headteacher who has been designated this role and is the Designated Lead for Safeguarding. 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, CEOP (Child Exploitation and Online Protection) and Childnet. The Chair and safeguarding governors annually check the security of the school's security settings.

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 (see Appendix), 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 PHSE.

eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT lessons.

- The school provides opportunities within a range of curriculum areas to teach about eSafety

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

- Pupils are aware of the need to ask an adult if they experience problems while using the internet.

eSafety Skills Development for Staff

- Our staff receive information and training on eSafety issues in the form of courses, staff meetings, INSET and visiting professionals.

- Details of the ongoing staff training programme can be found in the school office.

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

- The eSafety/social media policy will be introduced to staff at the start of each school year

- eSafety posters are displayed

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SRP or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident. Due to the age of our pupils, it is anticipated that incidents of cyber-bullying or deliberate racism within school would be extremely rare. However to track any such incidents and to record other concerns (e.g. children being exposed to, or using, inappropriate computer gaming or social network sites) a Record of Concern form is available in the school office. All such concerns should be reported to a member of the SLT and will be monitored by the DSL and DDSL.

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 eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

- Users are made aware of sanctions relating to the misuse or misconduct by the Headteacher.

Online safety (Annex C KCSIE 2016)

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;

- contact: being subjected to harmful online interaction with other users; and

- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filters and monitoring Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.88

The UK Safer Internet Centre has published guidance as to what “appropriate” might look like:

- UK Safer Internet Centre: appropriate filtering and monitoring

Guidance on e-security is available from the National Education Network-NEN. Buying advice for schools is available here: buying for schools.

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Staff training Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

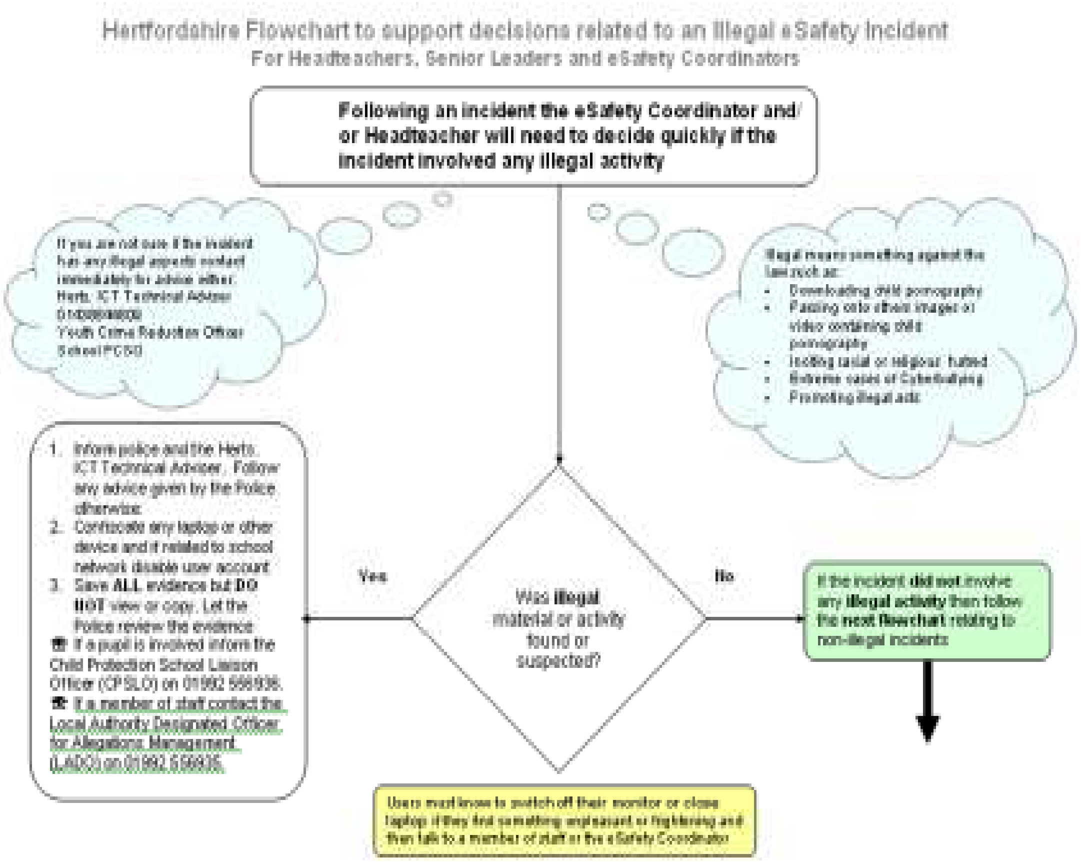
www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Flowcharts for Managing an eSafety Incident

- http://www.thegrid.org.uk/eservices/safety/research/incident.shtml)



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

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

If you are not sure if the incident has any illegal aspects contact immediately for advice either:
Herts. ICT Technical Advisor 01438844806
Youth Crime Reduction Officer
School PCSO

Illegal means something against the law such as:
- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

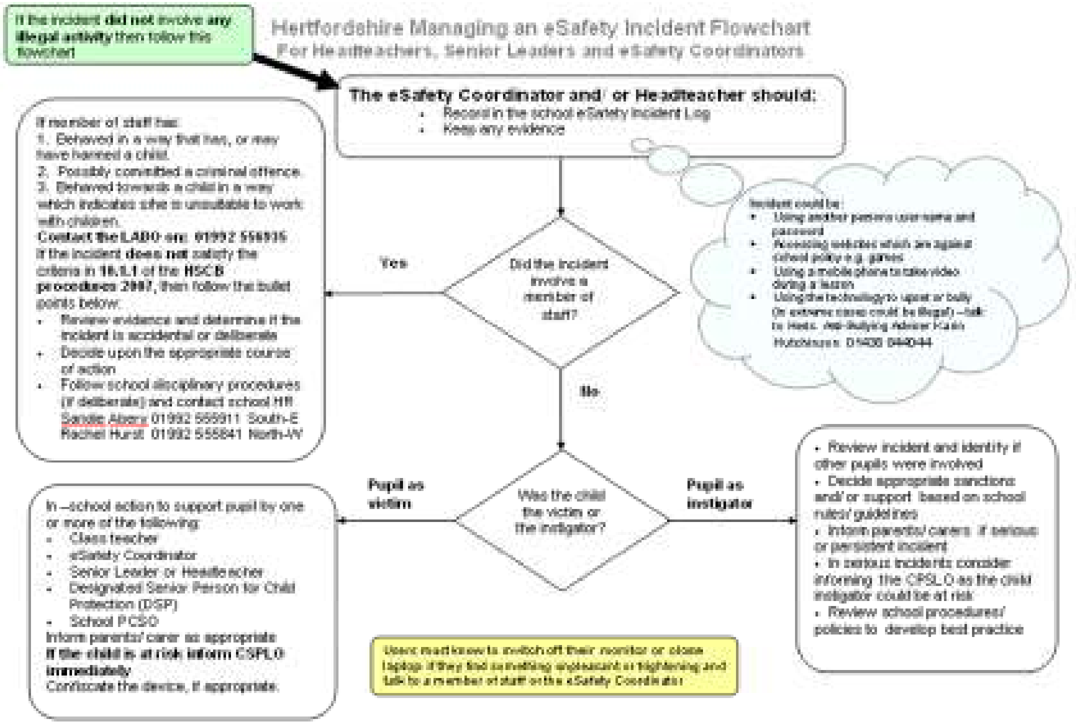
Was illegal material or activity found or suspected?

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

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.
☎ If a member of staff contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 556935.

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

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



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

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

The eSafety Coordinator and/ or Headteacher should:
- Record in the school eSafety Incident Log
- Keep any evidence

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

Did the incident involve a member of staff?

If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.
Contact the LADO on: 01992 556935
If the incident **does not** satisfy the criteria in **16.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:
- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR
Sandie Abery 01992 555911 South-E
Rachel Hurst 01992 555841 North-W

Was the child the victim or the instigator?

In –school action to support pupil by one or more of the following:
- Class teacher
- eSafety Coordinator
- Senior Leader 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.

- 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

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

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Hertfordshire Grid for Learning (HGfL) 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 students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use

- 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 or confidential information or disseminate such information in any way that may compromise its intended restricted audience

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

- On-line gambling or gaming is not allowed

- It is at the Head teacher's discretion on 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 LA's web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml

- Goldfield 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 are aware that school based email and internet activity can be monitored and explored further if required

- If staff 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. Pupils are reminded that if anything on screen worries or scares them, they are to tell a staff member.

- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

If there are any issues related to viruses or anti-virus software, the network manager should be informed by noting in the ICT Book in the staffroom.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through participation in surveys and questionnaires.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar

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

  - Information and celebration evenings

  - Posters

  - Website/ Learning Platform postings

  - Newsletter items

  - Learning platform training

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child your password
- Passwords should be a minimum of six characters and be difficult to guess

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 and change or password 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 Management Information System (where appropriate) log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 60 minutes.
- Due consideration should be given when logging into the Learning Platform

to the browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of Anne Nolan and all staff and pupils are expected to comply with the policies at all times

- User accounts in the name of staff who leave the school and therefore no longer have authorized access to the school system, should be disabled to avoid so called “zombie accounts” presenting a security risk.

Personal or Sensitive Information

Protecting Personal or confidential 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 that you lock your screen before moving away from your computer to prevent unauthorized access to personal, sensitive or confidential information. Keep your screen display out of direct view of any third parties when accessing such information.

- Ensure that any information of this nature shared with authorized persons is accurate. Do not share such information with unauthorized persons.

- Ensure the security of such information contained in documents when faxed, scanned, copied or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

- You must not post on the internet personal or confidential information, or disseminate such information in any way that may compromise its intended restricted audience.

- Ensure hard copies of data are securely stored and disposed of after use.

Storing/Transferring Personal or confidential 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 or confidential data

- Ensure hard drives from machines no longer in service are removed, stored securely or are wiped clean

When using removable media for storing or transferring personal or confidential information

- Always consider if there is an alternative solution
- Only use recommended removable media
- Encrypt and password protect

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
- Keep all dail-up access information such as telephone numbers, logon IDs and PINs confidential
- If such information is written down, these documents should be stored securely and disguised to avoid unauthorized access
- Protect school information and data at all times. 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://connect.hertscc.gov.uk/connect/news/images/?view=connect**

- All parent are given the opportunity to opt out of the taking of images by staff and pupils.
- Staff and parent helpers 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 Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Separate parental permission will be sought before images are used in the press.

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

If a parent does not opt out on the form given to parents on entry to Goldfield their permission is given 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, ie exhibition promoting the school

This ‘opting out’ form is considered valid for the entire period that the child attends this school unless informed otherwise by the parents.

Parents/ carers may wish to ‘opt out’, in writing, at any time.

Pupils’ full 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.

Only the Web Manager has authority to upload to the site.

For further information relating to issues associated with School websites and the safe use of images in Hertfordshire schools, see

http://www.thegrid.org.uk/schoolweb/safety/index.shtml

http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

Storage of Images

- Images/ films of children are stored on the school’s network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff within the confines of the school network or other online school resource.
- Mrs C Rolph has the responsibility of deleting images when they are no longer required.
- The school reserves the right to archive images that may later be used to show the history of the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Headteacher, office manager and site manager. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspxSchool ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available

- Ensure that all ICT equipment that you use is kept physically secure

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- 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 or confidential information is disclosed to any unauthorised person

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware may be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use, the device must be switched to silent. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Servers

- Always keep servers in a locked and secure environment

- Limit access rights and password protect the server

- Existing servers should have security software installed appropriate to the machine's specification

- Backup tapes should be encrypted by appropriate software and must be stored in a fireproof container. Any back up media off site should be stored securely

- Data must be backed up regularly

- Remote backups should be automatically encrypted

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

Staff have been involved in making/ reviewing the Policy for ICT Acceptable Use through Governing Body meetings and staff meetings. Due to the age of our pupils, they have not been involved in its creation.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

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

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

eSafety Guidelines to be displayed throughout the School

These rules help us to stay safe on the internet

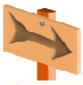
Think then Click

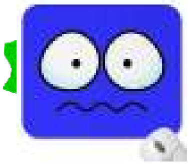
We only use the internet when a trusted adult is with us

We can click on links and buttons when we know what they do.

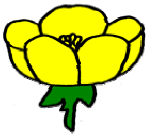
We can search the Internet with an adult.

We always ask if we get lost on the Internet.

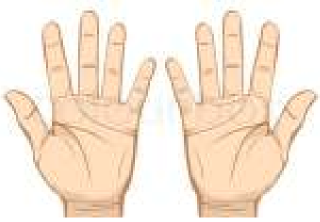




We always tell a trusted adult if we find something that worries us.



Our iPad Rules

	**Hold the iPad with two hands.**
	Always sit down when using the iPad.
	Turn the iPad's screen off when the teacher is talking.
	Be gentle when tapping the screen.
	Only use the app or website you have been asked to use.

Be Safe…. Be Responsible…. Be Respectful

Goldfield Pupil Acceptable Use Agreement / eSafety Rules

- I will always take care with ICT equipment and use it carefully.
- I will only use the programs and activities that my teacher has told me to.
- I will not tell other people my ICT passwords.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will find an adult to help me if I see anything that worries or frightens me.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will work co-operatively with other children sharing equipment fairly.
- I know that my use of ICT can be checked and that my parent may be contacted if a member of school staff is concerned about my eSafety.

Dear Parent/ Carer

Today has been internet Safety Day at Goldfield; the children have been taking part in activities introducing them to simple ways to keep safe while using the internet. ICT including the internet, e-mail and mobile technologies, play a vital role in teaching and learning and are now more easily accessible in the home. We expect all children to be safe and responsible when using any ICT.

We would like the children to share the information at home with you. 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 Caroline Rolph or Mrs Debbie Stevens.

For more information about internet safety please visit Childnet's parent support page www.childnet-int.org/ .

- - ✂ -

Parent/ carer signature
We have discussed this and ……………………………………………(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Goldfield Infants' and Nursery School.

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

Child's 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 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, governors and regular visitors are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher or IT Subject Leader.

- 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, 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, eg on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher, IT Subject Leader or SLT.
- 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 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 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 role or that of others into disrepute
- I will support and promote the school's e-Safety, Social Media and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- Staff: 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)

Position in School/JobTitle ……………………………………………………………………

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

SMILE and stay safe

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.

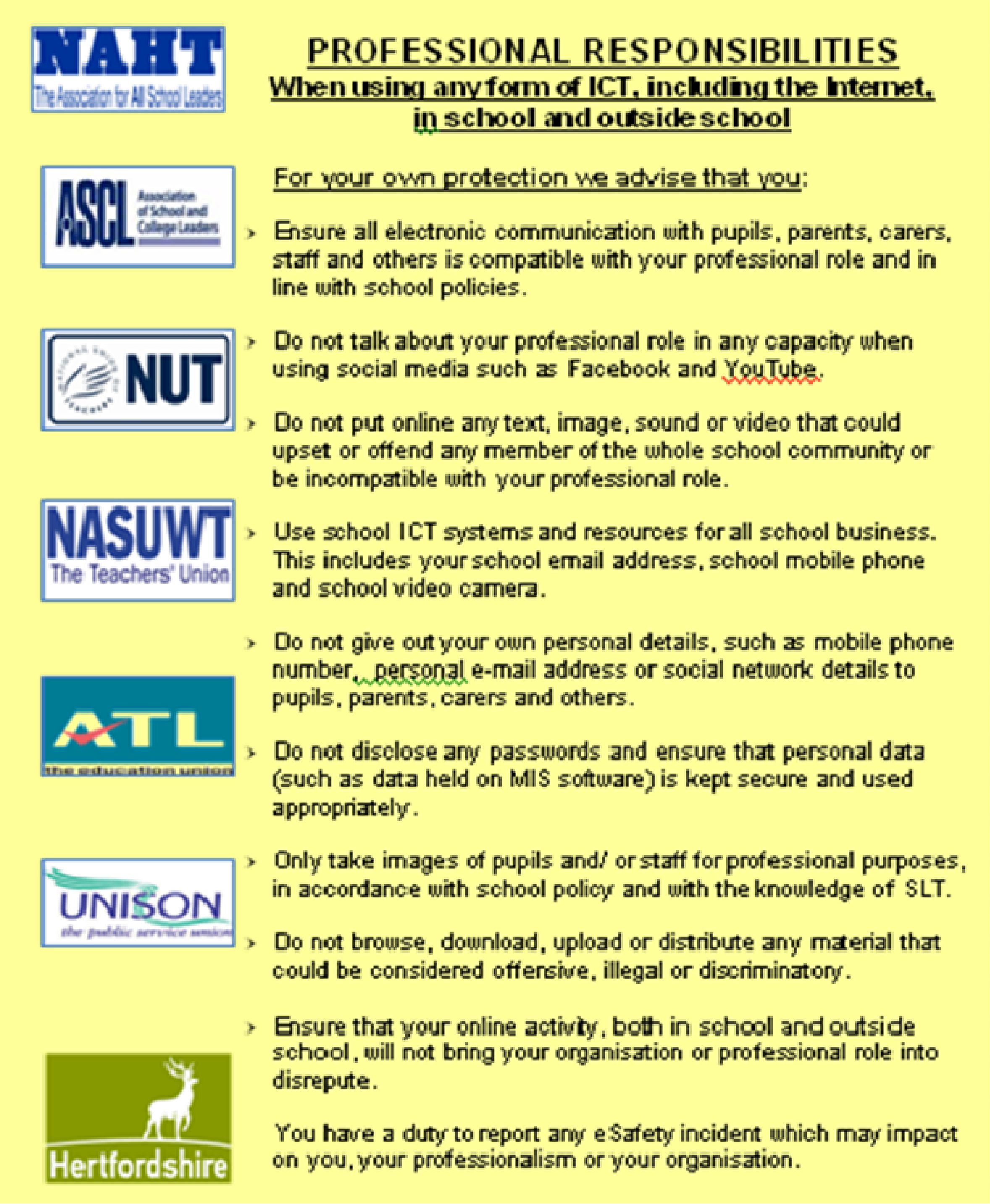
Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

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.

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.

NAHT
The Association for All School Leaders
ASCL Association of School and College Leaders
NUT
NASUWT The Teachers' Union
ATL the education union
UNISON the public service union
Hertfordshire

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 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.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 200

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