BROOKLAND INFANT AND NURSERY SCHOOL

eSAFETY

AND

DATA SECURITY

Guidance Policies for ICT Acceptable Use

This policy has been adapted from Herts for Learning's model eSafety & Data Security Policy

Version date: September 2016

Review date: January 2018

Signed: .... Chair of Governors

Signed: .... Headteacher

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- APPs
- E-mail, Instant Messaging and chat rooms
- Social media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and other gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio/Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (usually 13 years).

At Brookland Infant and Nursery School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

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

Monitoring

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 policy breach is grounds for disciplinary action in accordance with the school's 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 Office's (ICOs) new 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

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 Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individual in our school is the Headteacher.

Please also refer to the relevant section on Incident Reporting, e-Safety Incident log and Infringements.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (such as a memory stick) must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment
- Computers/laptops not routinely connected to the school network must be regularly given to the IT technician for an anti virus update
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The Local Authority guidance documents listed below:
http://www.thegrid.org.uk/info/dataprotection/index.shtml#data

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are made 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
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the sender before it is sent
- Anyone expecting a confidential or sensitive fax should ask the sender to notify them when it has been sent

Protective Marking of Official Information

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine official information.
- Optional descriptors can be used to distinguish specific type of information
- Use of descriptors is at an organisation's discretion
- Existing information does not need to be remarked

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'Official – Sensitive'.

Relevant Responsible Persons

Senior members of staff are familiar with information risks and the school's response. The Headteacher acts as the SIRO (Senior Information Risk Owner) and has the following responsibilities:

- leads on the information risk policy and risk assessment
- advises school staff on appropriate use of school technology
- acts 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.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off 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 or the school will do this before hardware is collected

- Disposal of any ICT equipment will conform to:
  - ❖ The Waste Electrical and Electronic Equipment Regulations 2006
  - ❖ The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
    http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
    http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
    http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
  - ❖ Data Protection Act 1998
    https://ico.org.uk/for-organisations/education/
  - ❖ Electricity at Work Regulations 1989
    http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

- The school's disposal record will include:
    - ❖ Date item disposed of
    - ❖ Authorisation for disposal, including:
        - ➢ verification of software licensing
        - ➢ any personal data likely to be held on the storage media? *
        - ➢ How it was disposed of eg waste, gift, sale
        - ➢ Name of person & / or organisation who received the disposed item

    ** if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.*

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information is 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

Information Commissioner website
https://ico.org.uk/

PC Disposal – SITSS Information
http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsibly online.

Managing e-Mail

- The school gives all teachers, governors and some support staff (if they want one) their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending e-mails to external organisations, parents or pupils are advised to copy (or blind copy) the Headteacher and/or admin account
- 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 Headteacher if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies refer to the Section 'Emailing Personal or Confidential information'
- Staff must use their own school e-mail account so that they are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising
- When ordering resources or booking events by e-mail staff should copy them to the headteacher/admin as appropriate

Receiving e-Mails

- Check e-mail regularly
- Activate 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source – always check with headteacher/office staff if in doubt
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

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

- ➢ 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.shtmle

Where it I not possible to use the above portal then:

- Obtain express consent from the Headteacher/Finance & Admin 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:
  - Encrypt and password protect – see: http://www.thegrid.org.uk/info/dataprotection/#securedata
  - Verify the details, including accurate e-mail address of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any 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

Equal Opportunities

Pupils with Additional Needs

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

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

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

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Headteacher is the eSafety co-ordinator in this school and is a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as HCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Headteacher 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 (Safeguarding), health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety in the Curriculum

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

The school provides opportunities within a range of curriculum areas to teach about eSafety. Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise as well as part of the eSafety curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety, and how they can promote the 'Stay Safe' online messages, in the form of memos, staff meetings, updates on Hertfordshire's 'Grid for Learning', and specific training etc.
- Details of the ongoing staff training programme can be found in the staff meeting minutes folder.
- 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 Co-ord).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up to date areas of concern.

Managing the School eSafety Messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used and eSafety posters will be prominently displayed.

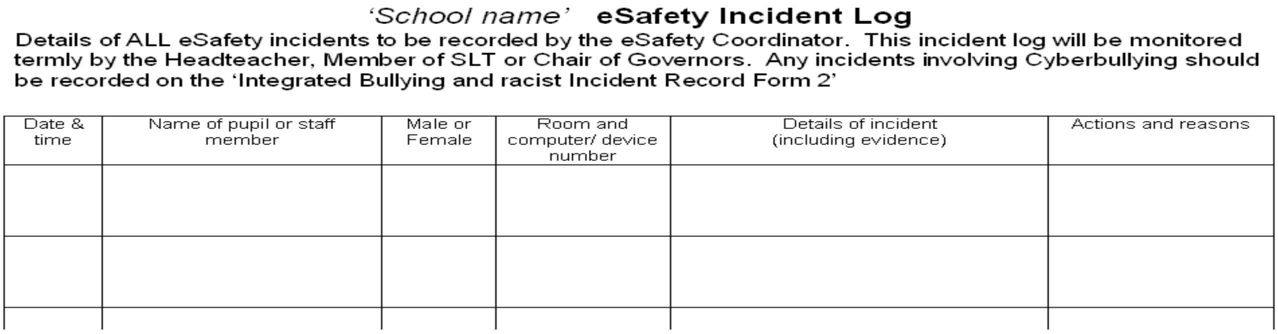
Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher.

eSafety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identifying trends or specific concerns.



'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

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

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the Headteacher. Incidents should be logged and the Hertfordshire Flowcharts for Managing an eSafety Incident should be followed.

Inappropriate Material

- All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher as the eSafety Co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, 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 in e-safety file)
- Users are made aware of sanctions relating to the misuse or misconduct through this policy and the Staff Handbook.

Flowcharts for Managing an eSafety Incident are available in the eSafety file in the school office or can be downloaded from:
http://www.thegrid.org.uk/eservices/safety/research/incident.shtml

Internet Access

The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All 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 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
- Raw image searches are discouraged when working with pupils
- If Internet research is set for home learning, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Staff must not reveal names of colleagues, pupils or others or any other confidential information acquired through their job on any social networking site or blog
- On-line gambling or gaming is not allowed

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

Infrastucture

- Our school subscribes to the HICS web filtering service and therefore has the benefit of monitored web activity. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- Brookland Infant and Nursery School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff are made aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Headteacher or teacher as appropriate
- The school accepts that it has the responsibility to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- Staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher/ICT subject leader
- If there are any issues related to viruses or anti-virus software, the Headteacher/Finance & Admin Manager should be informed and it should be logged for the attention of the IT Technician

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities.

However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school's Learning Platform or other systems approved by the Headteacher
- When signing up to online services that require the uploading of what could be deemed as **personal or sensitive data**, schools should check terms and conditions regarding the location of storage. Please see the Safe Harbor Agreement Statement http://www.thegrid.org.uk/info/dataprotection/#data

  Also: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Parental Involvement

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

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and if these images can be used in the public domain (eg on school website, school app, etc)
- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar
  - We will support the school's approach to on-line safety and not upload or add any text, images, sounds or videos that could upset or offend any member of the school community or bring the school name into disrepute
  - We will ensure that our online activity will not cause the school, staff, pupils or others distress or bring the school community into disrepute.

  - We will support the school's policy and help prevent our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (below 13 years in most cases)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - School's website
  - Newsletter items

Passwords and Password Security

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

Passwords

- Users should always use their own personal passwords
- Users should make sure they enter their personal passwords each time they logon and do not include passwords in any automated logon procedures
- Users should change temporary passwords at first logon
- Users should change passwords whenever there is any indication of possible system or password compromise
- Users should not record passwords or encryption keys on paper or in an unprotected file
- Users should only disclose their personal password to authorised ICT support staff when necessary, and never to anyone else and should ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Users should never tell a child or colleague their password
- If users are aware of a breach of security with their password or account they should immediately inform the Headteacher
- Passwords should contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ids and passwords for staff and pupils who have left the school will be removed from the system when no longer required

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. Staff are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety and Data Security Policy.
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 6pm.

- Due consideration should be given when logging into the school's learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff and pupils are expected to comply with the policies at all times.

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. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorised access

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

All staff must:

- Ensure that any school information accessed from their own PC or removable media equipment is kept secure
- Ensure that they lock their screen before moving away from their computer during their normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents they fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so
- Not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Removable media will be purchased with encryption
- Removable media will be stored securely
- Removable media that may hold personal data must be disposed of securely through the school office
- Hard drives from machines no longer in service will be removed and stored securely, wiped clean or destroyed

Remote Access

- Staff are responsible for all activity via their remote access facility
- Staff should only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems staff should keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- PINs should be selected to ensure that they are not easily guessed
- Staff should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Staff should protect school information and data at all times, including any printed material produced while using the remote access facility. Particular care should be taken when accessing 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.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication
- Any images taken with permission are the property of the school and should only be used in relation to school business.

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:

- for assessment purposes
- on the school web site/school app
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video/webcam
- on the school's learning platform or virtual learning environment
- in display material that may be used in the school's communal areas
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

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

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Headteacher or Office Manager has authority to upload to the website/school app.

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, class computers and laptops
- 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
- Class teachers are required to delete images from the network, class computers, laptops, etc, when the images are no longer required, when pupils leave their class, leave the school

Webcams and CCTV

We do not use publicly accessible webcams in school

Video Conferencing

The school does not use video conferencing at the present time and if it does so in the near future this would only involve staff.

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

School ICT Equipment

- All users are responsible for their activity undertaken on the school's ICT equipment
- The school keeps a log of ICT equipment issued to staff and records serial numbers as part of the school's inventory
- Visitors should not be allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the school's wireless facility
- Staff should ensure that all ICT equipment that they use is kept physically secure
- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- Staff should save their data on a frequent basis, ideally to the school's network. Staff are responsible for the backup and restoration of any of their data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PCs, laptops, USB memory sticks or other portable devices. If it is necessary to do so the local drive/memory stick must be encrypted
- A time locking screensaver is applied to all machines and user profiles
- Privately owned ICT equipment should not be used on the school network
- On termination of employment, resignation or transfer, all ICT equipment must be returned to the school
- Staff are responsible for ensuring that any information accessed from their 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 Headteacher
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

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

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting a 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 Headteacher or IT Co-ordinator, fully licensed and only carried out by the IT Technician

- 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 should be transported in its protective case if supplied

Mobile Technologies

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

Personal Mobile Devices (including phones)

- The school or setting allows staff to bring in personal mobile phones and devices for their own use during non-contact rest periods only.
- During contact time personal devices should be switched off and put away beyond use.
- Personal mobile devices should not be used around children, in particular photographs and video should only be taken on school issued devices. It is essential that staff do not put themselves at risk of allegations.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Under no circumstances does the school allow a member of staff to photograph or video children on their personal device.
- Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used for any aspect of school business (eg contacting parents, taking photographs and videos, tweeting and Facebook status updates.)
- 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
- Volunteer helpers sign an agreement which states that phones should not be used for any purpose whilst they are working in the school.

Any exception to the requirements above should be specifically approved by the headteacher on a case by case basis.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- The school provides mobile technologies such as phones, laptops, tablets and cameras for use in school and on offsite visits. Only these devices should be used for any aspect of school business (eg contacting parents, taking photographs and videos, tweeting and Facebook status updates). Unless agreed by the headteacher these devices should not be taken home and should be stored in a secure location in school.
- Staff should be mindful that photographs and video taken of colleagues during working hours and at staff events should not be shared without permission of all those concerned and the headteacher.
- School SIM cards must only be used in school provided devices.
- Personal use of school owned devices is prohibited unless specifically approved by the headteacher or equivalent, and in accordance with the finance policy of the school.
- Permission must be sought before any image or sound recordings are made on the school devices of any member of the school community. Current permissions for pupils are kept in the class register file and in the school office. Images and video of children should never be taken without having secured signed permission from the parent or carer.
- School devices containing personal information, including photographs and video of children, should not be taken off the premises, except where parental permission has agreed to staff using photographs and video for assessment purposes

Removable Media

If storing or transferring personal, sensitive, confidential or classified 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
- Always dispose of removable media securely

Servers

- Servers will be kept in a locked and secure environment if possible
- Access rights will be limited
- Servers will be password protected
- If back-up tapes are used then they will be encrypted by appropriate software
- Data will be backed up regularly
- Back-up media is not stored off-site
- The database server is backed-up remotely managed by SITSS (Herts for Learning Ltd)

Social Media – including Facebook and Twitter

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

- At the present time our school does not use Facebook or Twitter to communicate with parents and carers. If it is decided to use these in the future the Headteacher will be responsible for deciding who will be responsible for all postings and for monitoring responses
- Staff are not permitted to access their personal social media accounts using school equipment on site during school hours
- Staff, governors, 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, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, parents and carers are aware that their online behavior should at all times be compatible with UK law

Systems and Access

Staff using the school's network, systems, equipment etc:

- are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC
- should not allow any unauthorised person to use school ICT facilities and services that have been provided to them
- should only use their own personal logons, account IDs and passwords and should not allow them to be used by anyone else
- should keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information
- should ensure they lock their screen before moving away from their computer during their normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- should ensure that they log-off from the school's database (SIMS) as soon as they have finished using it
- should ensure that they log-off from the PC completely when they are going to be away from the computer for a long period of time
- should be careful to not introduce or propagate viruses
- must not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- should be aware that any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act

- should, where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

Telephone Services & School Mobile Phones

- Staff may make or receive personal telephone calls provided:
  - They are infrequent, kept as brief as possible and do not cause annoyance to others
  - They are not for profit or to premium rate services
  - They conform to this and other relevant HCC and school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Staff should remember that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

If staff have been issued with a school mobile phone they:

- are responsible for the security of their school mobile phone. They must always set the PIN code on their school mobile phone and do not leave it unattended and on display (especially in vehicles)
- must report the loss or theft of any school mobile phone equipment immediately as the school remains responsible for all call costs until the phone is reported lost or stolen
- must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it
- must not send text messages to premium rate services
- must reimburse the school for the cost of any personal use of their school mobile phone. This includes call charges incurred for incoming calls whilst abroad.

School SIM cards must only be used in school provided mobile phones. All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.

Writing and Reviewing this Policy

Staff Involvement in Policy Creation

Staff and governors have been involved in making/reviewing the Policy for ICT Acceptable Use through staff and governor meetings

Review Procedure

Staff and governors should discuss with the Headteacher any issues of eSafety that concerns them.

This policy will be reviewed regularly particularly when any relevant guidance changes and consideration given to the implications for future whole school development planning.

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

This policy has been adapted from the model Hertfordshire policy.

The final Policy was approved on 29th September 2016 by the governing body following consultation with staff and governors.

All existing staff and governors will be issued with a copy of this policy and new staff will receive a copy as part of their induction.

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use
Agreement / eSafety Rules

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

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 the Headteacher.

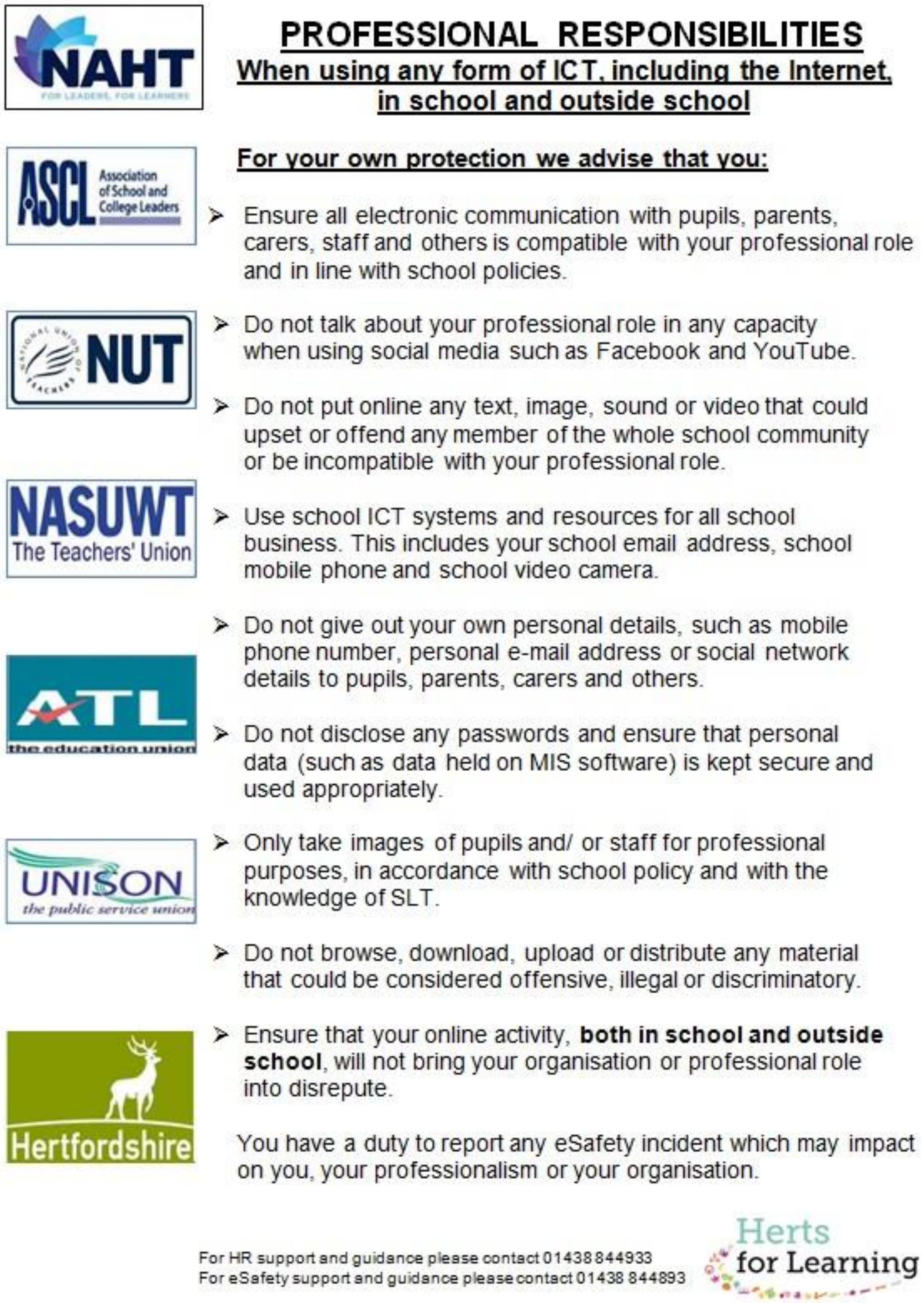
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or 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 IT technician
- 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 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.
- 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


NAHT
FOR LEADERS, FOR LEARNERS
ASCL Association of School and College Leaders
NUT
NATIONAL UNION OF TEACHERS
NASUWT The Teachers' Union
ATL the education union
UNISON the public service union
Hertfordshire

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

Herts for Learning