

Highwood Primary School



Promoting Resilience – Achieving Potential

ICT Acceptable Use Policy

June 2018



This policy has been impact assessed against protected characteristics (race, gender and disability) and no adverse impact has been identified.

Introduction

Information and Communications Technology (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, Highwood Primary School needs to build in the use of these technologies in order to arm our pupils with the skills to access life-long learning and employment. ICT covers a wide range of resources including both 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 our pupils are using both inside and outside of the classroom include:

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements (13 years in most cases). At Highwood Primary School, we understand the responsibility to educate our pupils about internet and eSafety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties; staff not directly involved in data handling are made aware of the risks and threats and how to minimise them. Both this policy and the ICT Acceptable Use Agreements (for all staff, governors, regular visitors[for regulated activities] and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask a member of the SLT. Any ICT authorised staff member will be happy to comply with this request. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the GDPR Regulations (May 2018), or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the GDPR Regulations (May 2018), the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

Please refer to the Data Breach Response Plan (May 2018), the Staff Code of Conduct and the ICT Acceptable Use Agreements. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

*See Data Breach Response Plan and Data Security Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher (Mrs Cathy Cox) and the eSafety Coordinator (Mr Steve Johnson). Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID user names and passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher and Data Protection Officer (Mr Darren Freeman). The eSafety Incident Log is completed alongside any information and paperwork required by the DPO in order to monitor and identify trends or specific concerns. 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.

Computer Viruses

All files downloaded from the internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used. Never interfere with any anti-virus software installed on school ICT equipment. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Security

The school gives relevant staff access to its Management Information System, with a unique username and password. It is the responsibility of everyone to keep passwords secure. Staff are aware of their responsibility when accessing school data. Staff have been issued with the relevant guidance documents and the ICT Acceptable Use Policy. Staff are asked 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/dataprotection/index.shtml#securedata>) Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - <http://www.thegrid.org.uk/info/traded/sitss/>). Staff are required to 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 their 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 copied, scanned or printed.

Relevant Responsible Persons:

The School Information Risk Officer (SIRO) at Highwood Primary School is the Headteacher (Mrs Cathy Cox).

The SIRO:

- 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 Data Protection Officer (DPO) at Highwood Primary School is Mr Darren Freeman (Governor) – See Data Security Policy for more details of responsibilities.

The Information Asset Owner (IAO) at Highwood Primary School is the HR and Contracts Manager (Mrs Paula Ladyman).

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

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

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

However, all staff must be clear that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

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

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

GDPR Regulations (May 2018)

<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
- If personal data is likely to be held on the storage media it will be over written multiple times to ensure the data is irretrievably destroyed
- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations
Environment Agency web site

Introduction

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

The Waste Electrical and Electronic Equipment Regulations 2006

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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

Information Commissioner website

<https://ico.org.uk/>

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

E-mail

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

Managing e-mail

The school gives all staff 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. All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. E-mails created or received as part of a member of staff's school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their 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
- Inform the ICT Manager or their line manager if they receive an offensive e-mail
- However the school e-mail account is accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies staff should refer to the Section
- e-mailing Personal, Sensitive, Confidential or Classified **Information**
- Use their 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
- Check e-mail accounts regularly
- Activate the 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; Consult the network manager first

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

Where a member of staff concludes that e-mail must be used to transmit such data they must:

- Obtain express consent from the line 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
- Not copy or forward the e-mail to any more recipients than is absolutely necessary
- Not send the information to any person whose details have not been separately verified (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)
- Not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt OR: Use Hertsfx or Schools fx, Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely <http://www.thegrid.org.uk/eservices/schoolsfx.shtml>

Equal Opportunities -Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools ICT Acceptable Use Agreements. 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 and young people.

Internet Safety - eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Mr Steve Johnson who has been designated this role as IT Manager. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Safeguarding, Health and Safety, Behaviour and Anti-Bullying. It is also linked to the Home School Agreement which is signed annually by parents/carers and by KS2 pupils.

In addition, 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 it.

- The school has a framework for teaching internet skills in Computing/ICT lessons
- 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 and as part of the eSafety curriculum

- Pupils are informed about the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages
- 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-ordinator)
- 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. The ICT Acceptable Use Agreement will be introduced to the pupils at the start of each school year and eSafety posters are prominently displayed. The key eSafety advice is promoted widely through school displays, newsletters, class activities and staff are encouraged to promote participation in Safer Internet Day every February.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher or member of the SLT. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart) Users are made aware of sanctions relating to the misuse or misconduct through the Code of Conduct

Flowcharts for Managing an eSafety Incident

See Appendix 4

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

<http://www.thegrid.org.uk/eservices/safety/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 internet use through the HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity. Staff will preview any recommended sites, online services, software and apps before use. Searching for images through open search engines is discouraged when working with pupils. If internet research is set for 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 the intended restricted audience
- Staff must not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online application
- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the IT manager or teacher for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from their teacher
- If there are any issues related to viruses or anti-virus software, the network manager should be informed

Infrastructure

Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded. School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to

<http://www.thegrid.org.uk/eservices/safety/filtered.shtml>. SITTS has access to all passwords and remote access. The SITTS system puts blocks in place and identifies unacceptable use.

Highwood School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998 and GDPR (May 2018), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school does not allow access to social networking and online games websites to pupils in school. Pupils are advised to be cautious when not at school about the information given by others on such websites, for example users not being who they say they are. Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online. Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests). Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals. Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online. Our pupils are asked to report any incidents of Cyberbullying to the school. Staff may only create blogs, wikis or other online areas in order to communicate with pupils using school software approved by the Headteacher.

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored <http://www.coppa.org/comply.htm>

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through Parentview meetings and questionnaires. Parents/carers are asked to read through and sign the Home School Agreement and ICT Acceptable Use Agreements annually which both clearly state the policies adhered to by the school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website). Parents/carers can opt out of this agreement at any time. The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Newsletters and information meetings
- School website information
- Posters

Passwords and Password Security

Users are provided with an individual network and email, log-in username. All users read and sign an ICT Acceptable Use Agreement to demonstrate that they have understood the school's ICT Acceptable Use Policy and Data Security Policy. User ID and passwords for staff and pupils who have left the school are removed from the system on their last working day. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security. All staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems, including ensuring that passwords are not shared and are changed every 3 months. 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 6:00pm for devices that are standing idle and 9:00pm for devices that are in use after 6:00pm. In our school, all ICT password policies are the responsibility of Nick Cronin (SITTS) and all staff and pupils are expected to comply with the policies at all times.

Staff should;

- refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>
- always use their personal passwords
- enter a personal passwords at each logon
- not include passwords in any automated logon procedures

- change temporary passwords at first logon
- change passwords whenever there is any indication of possible system or password compromise
- not record passwords or encryption keys on paper or in an unprotected file
- only disclose 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
- not tell a child or colleague their password
- report any breach of security or suspected breach of security with passwords or account information immediately
- use passwords that contain a minimum of six characters and be difficult to guess
- use passwords that contain a mixture of upper and lowercase letters, numbers and symbols

Pupils are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others

Protecting Personal, Sensitive, Confidential and Classified Information – Data Security

*Please read in conjunction with the Data Security Policy

Staff must:

- ensure that any school information accessed a school PC or removable media equipment is kept secure, and remove any portable media from computers when not attended
- ensure screens are locked before moving away from the computer during the normal working day to prevent unauthorised access
- ensure the accuracy of any personal, sensitive, confidential and classified information disclosed or shared with others (this should only be on a 'need to know basis')
- 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 copied, scanned or printed.
- only download personal data from systems if expressly authorised to do so by the line manager
- 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 screen displays out of direct view of any third parties when 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

Staff must:

- ensure removable media does not contain children's personal data
- store all removable media securely
- ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Please refer to the document on the grid for guidance on How to Encrypt Files

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

Remote Access

Staff are responsible for all activity via the remote access facility. The remote access facility used by staff at Highwood is Herts for Learning – Login Anywhere Remote Access (lara). Staff must only use equipment with an appropriate level of security for remote access. To prevent unauthorised access to school systems all login information and passwords must be kept confidential and not disclosed to anyone. When accessing the school system via remote access staff must protect school information and data at all times, including any printed material produced while using the remote access facility.

Safe Use of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. HCC guidance can be found: <http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse>

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. SLT are permitted to use school equipment (iphones/ipads) and personal cameras 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. Staff are invited to withdraw permission for images of all staff who work at the school to be used in displays and shared folders on an individual basis.

Publishing Pupil's Images and Work

On a child's entry to the school and every subsequent September, all parents/carers will be asked to give permission for the school to use their child's work/photos for educational purposes such as:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the ICT Manager or members of the SLT have authority to upload to the internet.

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

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

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

Storage of Images

Images/ films of children are stored on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource. The ICT Manager has the responsibility of deleting the images when they are no longer required, or as soon as possible after the pupil has left the school.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the Site Manager, Office staff and SLT. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance <https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/>. We do not use publicly accessible webcams in school. Webcams will not be used for broadcast on the internet without prior parental consent. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices. For

further information relating to webcams and CCTV, please see:

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

Video Conferencing

Highwood Primary School does not currently use video conferencing; if it is to be used the following paragraph will apply.

Permission will be sought from parents and carers if their children are involved in video conferences with end-points outside of the school. All pupils will be supervised by a member of staff when video conferencing. The school will keep a record of video conferences, including date, time and participants. Approval from the Headteacher will be sought prior to all video conferences within school to end-points beyond the school. No part of any video conference will be recorded in any medium without the written consent of those taking part.

Additional points to consider:

Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) checked. Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

For further information and guidance relating to Video Conferencing, please see:

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

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

Guidelines for staff

- Do not allow visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to the ICT Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

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 except in exceptional circumstances as agreed by the Headteacher. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey. Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, 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 allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

Upper Key Stage Two pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. Pupils must drop them off at the office when they arrive at school and pick them up at the end of the school day.

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

The sending of inappropriate text messages between any member of the school community is not allowed. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

The sending of inappropriate text messages between any member of the school community is not allowed. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community. Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used. Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Telephone Services

Staff may make or receive personal telephone calls provided:

- they are infrequent, kept as brief as possible, do not cause annoyance to others and are conducted out of sight of pupils
- they are not for profit or to premium rate services
- they conform to this and other relevant HCC and school policies.
- be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- ensure that incoming telephone calls can be handled at all times
- follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat.

School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

Social Media, including Facebook, WhatsApp and Twitter

Facebook, WhatsApp Twitter and other forms of social media are increasingly becoming an important part of our daily lives. Our school uses Twitter to communicate with parents and carers. Members of the SLT are responsible for all postings and monitors responses from others. Staff are not permitted to access their personal social media accounts using school equipment at school during school hours. Staff are able to setup accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media. Pupils are not permitted to access their social media accounts whilst at school. Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever. Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Appendix 1: Further help and support – for reference

Your organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998 and the GDPR (May 2018). For more information visit the website of the Information Commissioner's Office <https://ico.org.uk/>

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

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

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

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

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

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

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2014. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision –

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

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

Data Protection Act 1998 – N.B. Refer to GDPR (May 2018)

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

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

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

Human Rights Act 1998 <http://www.hms.gov.uk/acts/acts1998/19980042.htm>

Racial and Religious Hatred Act 2006 - It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003 - The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127) - Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to

imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3) - Regardless of an individual's motivation, the Act makes it a criminal offence to gain: access to computer files or software without permission (for example using another person's password to access files), unauthorised access, as above, in order to commit a further criminal act (such as fraud), impair the operation of a computer or program, UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1) - This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988 - Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29) - This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1) - It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964 - Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 2000

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

Appendix 2: Smile and Stay Safe Poster: eSafety guidelines to be displayed throughout the school



- Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.
- Never reply to ASL (age, sex, location)
- Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you
- Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'
- Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply



Highwood Primary School Acceptable Use Agreement: Key Stage Two

I agree that:

- I will only use ICT in school for school purposes or when given permission by an adult (e.g. in Golden Time)
- I will only open/delete my own files
- I will agree with my partner if I want to edit or delete a document we have worked on together
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately 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, send or post my image
- 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 internet safety and not deliberately 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

Signed

**Appendix 4: Letter to
parents/carers**



Highwood Primary School
Mead Way, Bushey, Watford, Hertfordshire, WD23 2AW
Tel: 01923 256210 E-mail: admin@highwood.herts.sch.uk

Cathy Cox - Head Teacher

Date:

Dear Parent/ Carer

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

Please read and discuss these ICT Acceptable Use 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 your child's class teacher or Mr Steve Johnson (IT Manager).

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

Kind regards,
Mrs Cathy Cox (Head teacher)



ICT Acceptable Use Agreement Reply Slip

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

Parent/ Carer Signature

Class Date

Appendix 5: Acceptable Use Agreement for Staff and Governors



Highwood Primary School Staff and Governor ICT Acceptable Use Agreement (Academic Year 2019 - 20)

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 agreement 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 agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher.

- I confirm that I have read, understood and will adhere to the school's ICT Acceptable Use Policy and Data Security Policy
- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal 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 or accessed remotely (via the LARA portal only). Personal or sensitive data **must not** be taken off site without prior permission of the Headteacher
- I will not install any hardware or software without permission from the Head teacher or IT Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I understand that images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher
- I will support the school approach to internet safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights
- I will not discuss any school business on any social media website and 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 help pupils to be safe and responsible in their use of ICT and related technologies

I understand that this agreement forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this agreement and support the safe and secure use of ICT at Highwood.

Signature Date

Full Name(printed)

Job title

Appendix 6: Staff Professional Responsibilities



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



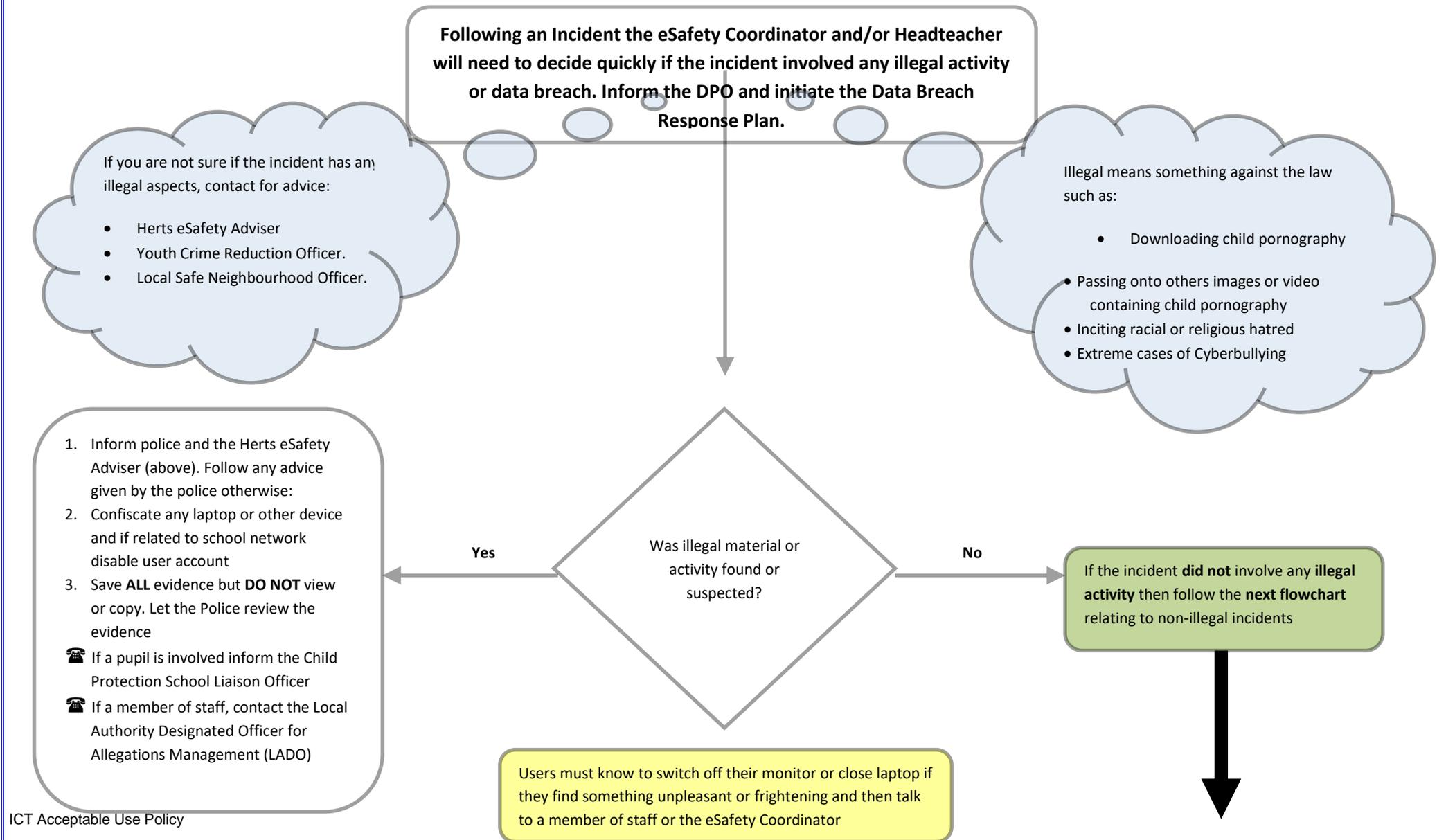
For your own protection we advise that you:



- 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.

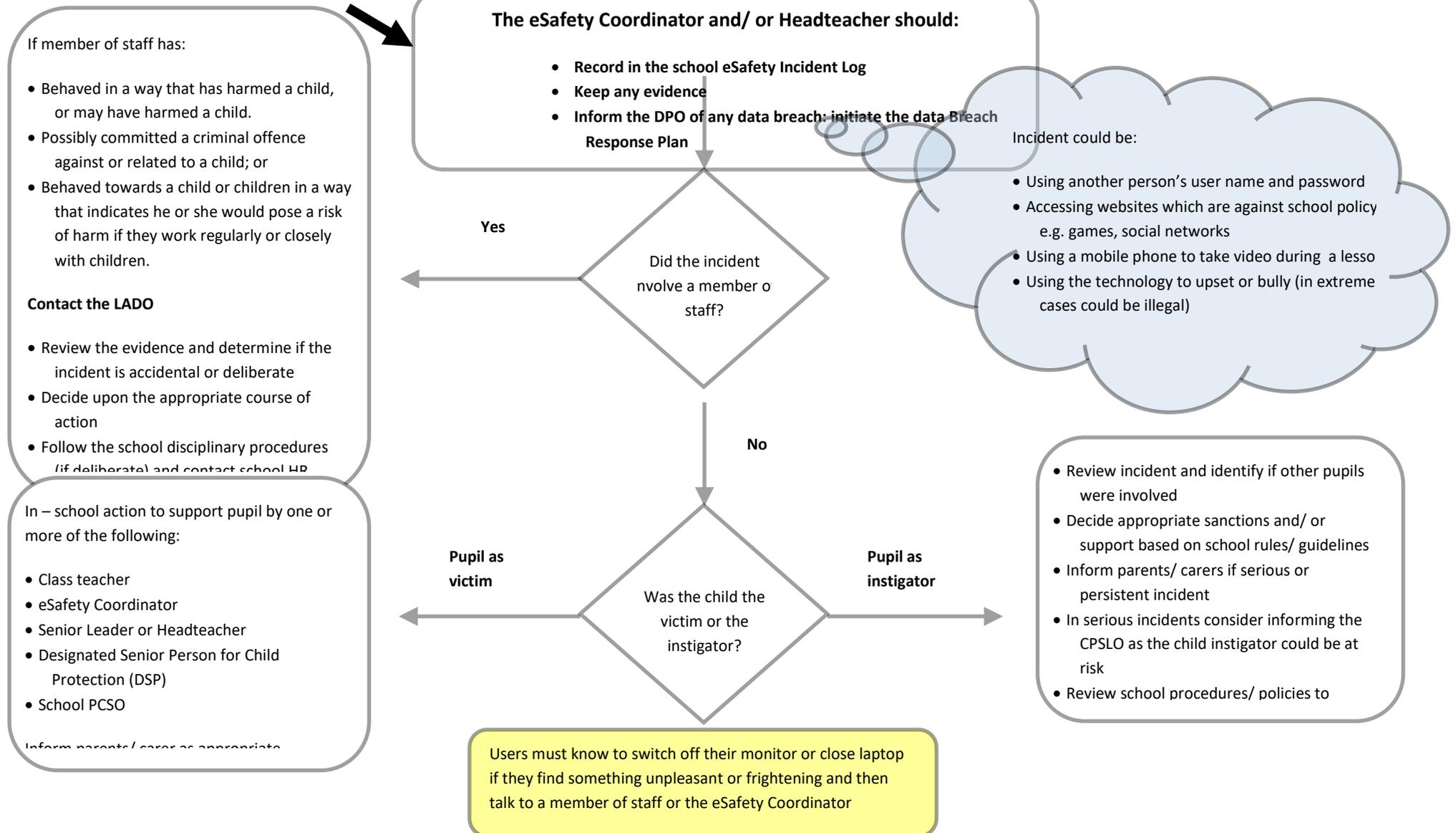
You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

Appendix 9 Hertfordshire Flowchart to support decisions related to an illegal eSafety Incident For Headteachers, Senior Leaders and eSafety Coordinators



Appendix 10: Hertfordshire Managing an eSafety Incident Flowchart

For Headteachers, Senior Leaders and eSafety Coordinators



Appendix 11: Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and eSafety Coordinator

The HT or Chair of Governors can be the single point of contact to coordinate responses.

Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
 - You have become aware of discussions taking place online...
 - You want to discuss this
 - You have an open door policy so disappointed they did not approach you first
 - They have signed the Home School Agreement which clearly states ...
 - Request the offending material be removed.
- If this does not solve the problem:
 - Consider involving the Chair of Governors

All incidents should be reported to the Headteacher and/ or Governors who will:

- Record in the school eSafety Incident Log
- Inform the DPO and initiate the Data Breach Response Plan
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider including the Chair of Governors and/ or reporting the incident to the Governing Body

If you feel unable to report an incident to your HT you could talk to a member of SLT or contact HfL

Staff as instigator

Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools eSafety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Pupils as instigators

Follow some of the steps below:

- Identify the pupil involved
 - Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.
- If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account
- Take appropriate actions in line with school policies/ rules
 - Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team

Further contact to support staff include:

- District School Effectiveness Adviser DSEA/ Schools eSafety Adviser/ Schools HR/ School Governance/ Hertfordshire Police/ HCC Legal Helpline 01992 555536
- The member of staff may also wish to take advice from their union

