West Horndon
Primary School

IT Security, Information Procedures & E-Safety

Staff consultation:

Adopted by Governors: E.P. Sanders

Implemented: 14/10/15

Due for Review: 14/1/18.

8th September 2015 Theresa Walker

IT Security, Information Procedures & E-Safety

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Essex County Council (ECC) 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 Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT and all other policy non-compliance must be immediately reported to the school's Head teacher.
See flowcharts (appendix 4) for dealing with both illegal and non-illegal incidents
An example security breach report can be found on the Essex Schools Infolink>Information Governance>Security Breaches.

Computer Viruses

1. All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB) must be checked for any viruses using school provided anti-virus software before using them
2. Never interfere with any anti-virus software installed on school ICT equipment that you use
3. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and notify your ICT subject leader who can conact the 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 school follows Essex guidelines and other guidance documents listed below
The safe use of new technologies - Ofsted
http://www.egfl.org/egfl/custom/files_uploaded/uploaded_resources/5723/safe_use_of_new_technologies_ofsted.pdf
e-Safety Audit Tool - Information for Governors, Management and Teachers
http://www.nen.gov.uk/hot_topic

Security

IT Security, Information Procedures & E-Safety

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the EGfL website
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- 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 copied, scanned or printed.

Information Asset Owner (IAO)

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

Information Asset Owners are the Office Manager and senior leadership team

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

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

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

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through our IT support provider. Hard drives containing personal data will be wiped.

8th September 2015 Theresa Walker

- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm
The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal in the asset management list
The school's disposal record will include:

- Date item disposed of
- Authorisation for disposal from Headteacher/ICT Co-ordinator:
- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item
- Date hard drive (if personal data) wiped by the school

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
http://www.ico.gov.uk/
Data Protection Act – data protection guide, including the 8 principles
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

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 good network etiquette; 'netiquette'. Pupils will experience sending and receiving e-mails as part of their ICT lessons via school's VLE eSchools.

Managing e-Mail

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

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All children use an egfl e-mail address
- The forwarding of chain letters is not permitted in school.
- All pupil e-mail users are expected to adhere to the general rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the Headteacher if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the computing curriculum
- However staff access 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 e-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

IT Security, Information Procedures & E-Safety

Receiving e-Mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail - **e-mailing confidential data is not recommended and should be avoided wherever possible.** the use of Hotmail, BTinternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

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

- Obtain express consent from your manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email 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 anybody/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) – preferably by telephone
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

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

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

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 schools' eSafety rules.

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

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

eSafety - Roles and Responsibilities

West Horndon Primary School takes the safety of all children and adults very seriously. This policy is written to protect all pupils and adults as well as develop skills that are required when communicating and using technology properly, keeping safe and secure, and acting with respect for others. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience. eSafety displays will be prominent and referred to effectively.

At West Horndon Primary School we believe that E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. E-safety is a focus in all areas of the curriculum and teachers reinforce e-safety messages across the curriculum. This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, behaviour and anti-bullying as well as forming part of the computing and PSHE curriculum.

E-Safety in the curriculum

The responsibility for eSafety co-ordination in this school is managed by the Computing Subject Leader and Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinators to keep abreast of current issues and guidance through organisations such ECC, CEOP (Child Exploitation and Online Protection) and Childnet. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and web-logs (blogs);
- **Internet research:** websites, search engines and web browsers;
- **Mobile phones and tablets**
- **Internet communications**: e-mail and IM;
- **Webcams and videoconferencing**: Skype;
- **Wireless games consoles**: PSP, Xbox, Playstation etc.

We believe that, in order to use information from the internet effectively, it is important for pupils to develop an understanding of the nature of the internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it is copyright. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

ICT provides pupils with opportunities to broaden and enhance their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

- Pupils will be taught to expect a wider range of content, both in level and in audience.
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium).

- When copying materials from the Web, pupils will be taught to observe copyright.
- Pupils will be made aware that the writer of an e-mail or the author of a webpage may not be the person claimed.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and PSHE lessons.

eSafety Skills Development for Staff

- All staff receive regular information and training on eSafety issues in the form of staff meetings for teachers and support staff
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Infrastructure

School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to essexccservicedesk. sen.uk@siemens-enterprise.com

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

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- 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 checked by the teacher first

If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing Social Networking Technologies

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 endeavours to deny access to social networking sites to pupils within school:

- All pupils are advised to be cautious about the information given by others on sites, 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 sites 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 such sites 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 profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs or wikis in order to communicate with pupils using the Learning Platforms approved by the Headteacher.

Parental Involvement

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

- Parents/ carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- Parents/ carers are expected to sign a Home School agreement
- The school disseminates information to parents relating to eSafety where appropriate in the form of;

o Information and celebration evenings
o Posters

o Website/ Learning Platform postings
o Newsletter items
o Learning platform training

Passwords and Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

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

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.

Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of **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 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 unauthorized access (Microsoft© advise every 42 days)

Further advice available **http://www.itgovernance.co.uk/**

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.

are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

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

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

ECC guidance can be found:
http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc

- 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 should avoid using personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. **Staff should use school cameras at all times**. Any images that are taken must be 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 the others, this includes when on field trips.

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- 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).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

IT Security, Information Procedures & E-Safety

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.

Further information relating to issues associated with School websites and the safe use of images in Essex schools on the Essex Schools Infolink http://esi.essexcc.gov.uk

Storage of Images

- Images/ films of children are stored on the school's network and audio visual Displays
- 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/ Learning Platform
- The Office Manager/ICT Co-ordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school

Video Conferencing and web cams

- All pupils are supervised by a member of staff when using video conferencing or web cam

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

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- 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 drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

- maintaining control of the allocation and transfer within their Unit
- recovering and returning equipment when no longer needed

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

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data. All activities carried out on School systems and hardware will be monitored in accordance with the general policy. Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey. 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. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

IT Security, Information Procedures & E-Safety

Personal Mobile Devices (including phones)

Pupils are not allowed to bring personal mobile devices/phones to school. In exceptional circumstances any at are should be handed in to the office at start of school.

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

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

- 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.

- The school allows staff to bring in personal mobile phones for own use. At all
- times they should be switched onto silent.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

Removable Media

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

- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software.

- Always keep servers in a secure environment
- Limit access rights to ensure the integrity of the standard build
- Always password protect the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back up tapes should be encrypted by appropriate software

IT Security, Information Procedures & E-Safety

- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Records should be kept of when and which patches have been applied
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength

Systems and Access

You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC 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 destroyed by the school.

Telephone Services

You may make or receive personal telephone calls provided:

1. They are infrequent, kept as brief as possible and do not cause annoyance to others
2. They are not for profit or to premium rate services
3. They conform to this and other relevant ECC and school policies.
4. School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
5. 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
6. Ensure that your incoming telephone calls can be handled at all times
7. Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office.

Data Protection

West Horndon Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;

3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

West Horndon Primary School Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

West Horndon Primary School

IT Security, Information Procedures & E-Safety

1. Requests for information must be made in writing; which includes email, and be addressed to Mr M O'Grady. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- ⍰f the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.

8th September 2015 Theresa Walker

Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Contacts
If you have any enquires in relation to this policy, please contact Mr O'Grady, Headteacher, at the school or telephone 01277 811741 who will also act as the contact point for any subject access requests.
Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

Writing and Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them. There will be an on-going opportunity for staff to discuss with the AIO any issue of data security that concerns them. This policy will be reviewed as it is deemed appropriate, but **no less frequently than every 2 years** so that consideration can be given to the implications for future whole school development planning and take account of the rapid developments in ICT. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. Current legislatation regarding data and freedom of information will be sought via the local authority to ensure the policy reflects best practice. The policy review will be undertaken by the Headteacher, or nominated representative

This policy should be read in conjunction with the Code of Conduct policy and the Freedom of Information procedures

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

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

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

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

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

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

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

access to computer files or software without permission (for example using another persons password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud)

impair the operation of a computer or program

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 200

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

Acknowledgement:

This policy is taken directly from the Essex County Council's Model policies for schools and adapted to suit the needs of West Horndon Primary School (eSafety and data security/guidance policies for ICT acceptable use). Essex County Council acknowledges and thanks Hertfordshire County Council for their help in producing this model policy.

IT Security, Information Procedures & E-Safety

Letter to accompany Primary Pupil Acceptable Use

Dear Parents and Carers,

At school we take the safety of our pupils very seriously including their safety while they access the internet, we want this approach to e---safety to spread to the home online environment too and we are therefore sharing with you some tips and resources to help you guide your children and help you keep up to date in a digital world. Here are a few tips to help you keep your children safe online: **Think u know (https://www.thinkuknow.co.uk/parents/Primary/)** is always a good place to start – you will see the report abuse button that your child will know about from school.

Another site that is helpful for parent controls is **UK Safer Internet Centre (http://www.saferinternet.org.uk/advice---and---resources/parents---and---carers)**.

This site advises you to take four steps:

1. Have on going conversations with your children about staying safe online
2. Use safety tools on social networks and other online services, e.g. Facebook privacy settings
3. Decide if you want to use parental controls on your home internet
4. Understand devices and the parental control tools they offer in our Parents' Guide to Technology Digital Parenting is another useful website to look at – http://www.pitda.co.uk/

There are three areas to think about:
WHO your child is talking to,
WHAT they're doing, and
WHERE they're going online

Digital Parenting also advises you to set "ground rules" by making your own family IT policy.

Create your own Family IT policy --- Ideas for the Under 5's

The big issues
Create boundaries and rules for the amount of time your son or daughter can spend online. It's never too early to start putting limits into place.
The basics
Choose an appropriate homepage on your family computer or tablet – for example, bbc.co.uk/cbeebies
Worth Checking
The educational apps, games and TV shows on offer for pre---school children, and the age ratings and descriptions for them.
Talk it through

IT Security, Information Procedures & E-Safety

Share your technology rules with grandparents, babysitters and older siblings, so that they stick to them when they look after your child or use the family computer.

And finally…..

The rules and conversation you have now will set the tone for your child's internet use as they get older. Please do not hesitate to contact me if you have any concerns or questions about keeping your child safe online.

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

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on request.

Parent/ carer signature

We have discussed this and ……………………………………………(child name) agrees
to follow the eSafety rules and to support the safe use of ICT at West Horndon Primary School.

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

Class ……………………………… Date ……………………………

West Horndon Primary School

IT Security, Information Procedures & E-Safety

Acceptable Use Agreement: Pupils – West Horndon Primary School

Primary Pupil Acceptable Use

Agreement / eSafety Rules

- I will only use ICT in school for school purposes.

- I will only use my own school e-mail address (eSchools) when e-mailing.

- I will only open e-mail 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 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 details such as my name, phone number or home address or internet passwords.

- I will not arrange to meet someone 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 know that my use of ICT can be checked and that my parent/ carer can be contacted if a member of school staff is concerned for my safety.

West Horndon Primary School

IT Security, Information Procedures & E-Safety

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupil and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed

Pupil:	***Class:***
Pupil's Agreement • I have read and I understand the school e-Safety Rules • I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times • I know that network and Internet access may be monitored.	
Signed:	***Date:***
Parent's Consent for Web Publication of Work and Photographs I agree that my son/daughters work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupils names **Parent's Consent for Internet Access** I have read and understood the school e-safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities. I will not take and then share online, photographs of other children (or staff) at school events without permission.	
Signed:	***Date:***
Please print name:	
Please complete, sign and return to **Theresa Walker**	

IT Security, Information Procedures & E-Safety

E-safety agreement form: parents and carers

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment (eSchools) ✓
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. ✓

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me. ✓

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this. ✓

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities. ✓

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose. ✓

I will not take and then share online, photographs of other children (or staff) at school events without permission. ✓

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. ✓

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. ✓

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns. ✓

My daughter / son name(s): ________________________________

Parent / guardian signature: __________________________

Date: ___/___/___

West Horndon Primary School

IT Security, Information Procedures & E-Safety

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

8th September 2015 Theresa Walker

West Horndon Primary School

IT Security, Information Procedures & E-Safety

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

8th September 2015 Theresa Walker

IT Security, Information Procedures & E-Safety

West Horndon Primary School	**Name of School**	**West Horndon Primary School**
	AUP review Date	
	Date of next Review	
	Who reviewed this AUP?	**Theresa Walker**

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system for any school business.
- I will only use the approved email system: eSchools, Mail365 West Horndon and school approved communication systems such as eSchools text to parents with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Computing Technician / Matt O'Grady (Headteacher).

IT Security, Information Procedures & E-Safety

- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system (Winpool drive) within school.
- I will follow the school's policy on use of mobile phones / devices at school (see code of conduct).
- I will use the school's Learning Platform (eSchools) in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer, laptop or tablet loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Matt O'Grady/Eileen Thorn/Julia Bolton (child protection officer / appropriate senior member of staff) if I feel the behaviour of any child may be a cause for concern.
- I will only use any LA system I have access to in accordance with their policies.

IT Security, Information Procedures & E-Safety

- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's e-safety and digital literacy curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ....Date......................................

Full Name .... (printed)

Job title / Role ....

Authorised Signature (Head Teacher / Deputy)

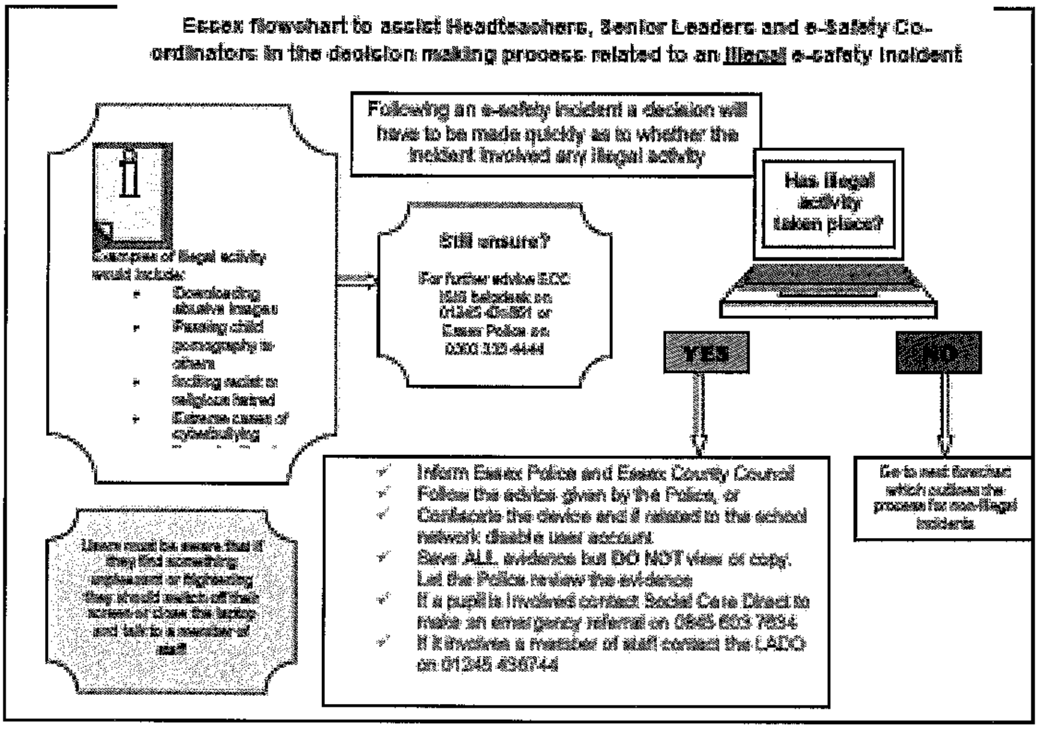
I approve this user to be set-up on the school systems relevant to their role

Signature .... Date...

Full Name .... (printed)

IT Security, Information Procedures & E-Safety

EssexWorks.
For a better quality of life



Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Has illegal activity taken place?

Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying

Still unsure?

For further advice ECC ISIS helpdesk on 01245 436691 or Essex Police on 0300 333 4444

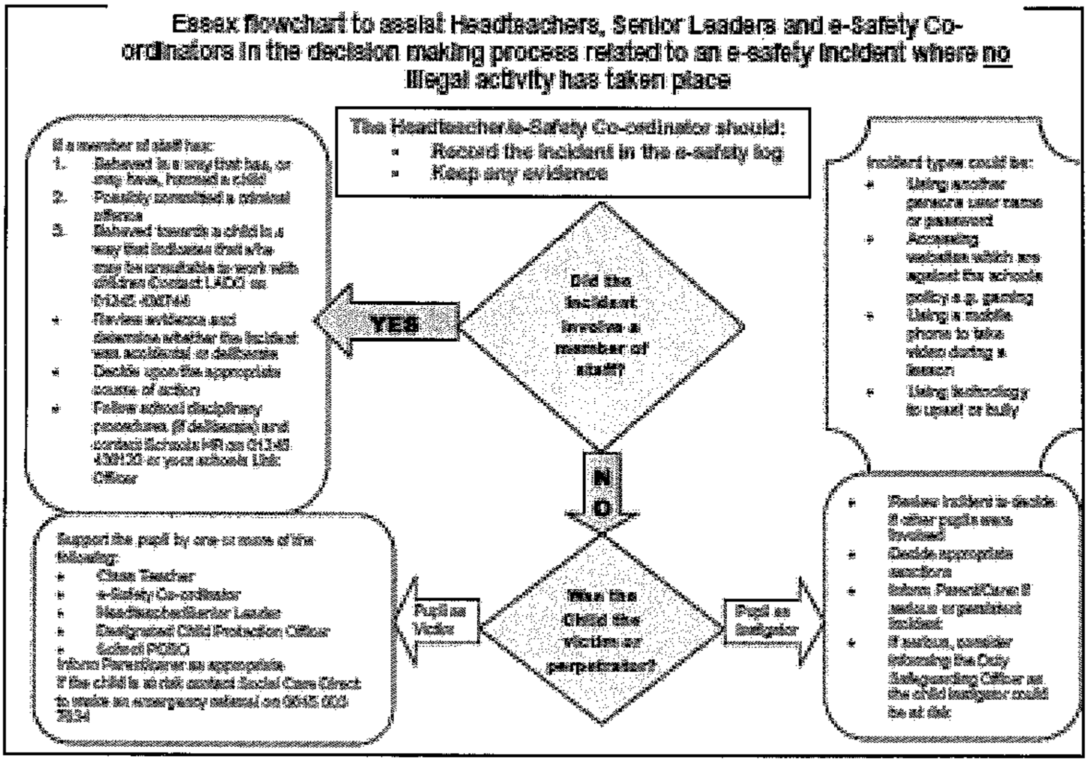
YES

NO

- ✓ Inform Essex Police and Essex County Council
- ✓ Follow the advice given by the Police, or
- ✓ Confiscate the device and if related to the school network disable user account
- ✓ Save ALL evidence but DO NOT view or copy. Let the Police review the evidence
- ✓ If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
- ✓ If it involves a member of staff contact the LADO on 01245 436744

Go to next flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff



Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place

The Headteacher/e-Safety Co-ordinator should:

- Record the incident in the e-safety log
- Keep any evidence

Did the incident involve a member of staff?

YES

If a member of staff has:

1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children Contact LADO on 01245 436744

- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer

Incident types could be:

- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

NO

Was the Child the victim or perpetrator?

Pupil as Victim

Support the pupil by one or more of the following:

- Class Teacher
- e-Safety Co-ordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- School PCSO

Inform Parent/Carer as appropriate.
If the child is at risk contact Social Care Direct to make an emergency referral on 0845 603 7634

Pupil as Instigator

- Review incident to decide if other pupils were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

Essex County Council