Lodge Farm Primary School
Online Safety and Data Security Policy

Author:	Claire Penfold
Role:	Online Safety Coordinator
Date of issue:	September 2017
Review date:	September 2019

Contents	Page

Writing and Reviewing this Policy

This policy sets out the ways in which **Lodge Farm Primary School** will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of online safety;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Online Safety and Data Security Policy through staff meetings, governor meetings, school council and pupil voice

Review Procedure

There will be on-going opportunities for staff to discuss with the online safety coordinator any online safety issue that concerns them

There will be on-going opportunities for staff to discuss with the Headteacher any issue of data security that concerns them

This policy will be reviewed every 2 years and consideration will be given to the implications for future whole school development planning

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

This Online Safety and Data Security policy has been read, amended and approved by the staff, head teacher and governors on _____

The next review date is: **September 2019**

Scope of policy

This policy applies to all members of the school community of **Lodge Farm Primary School**, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

Introduction

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

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

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

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

At ***Lodge Farm Primary School,*** we understand the responsibility to educate our pupils on Online Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and 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 your 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 and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
Both this policy and the Acceptable Use Agreement (for all staff, governors, 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).

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community.

The online safety coordinator will work with the Headteacher, also the designated Child Protection Coordinator, to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

All staff, governors, pupils, parents and carers will read and sign an Acceptable Use Agreement to show they fully understand their responsibilities with regards to acceptable use of ICT technologies and online safety. The AUAs can be found in Appendix 1.

Role	Responsibility
Governors	• Ensure that the school follows all current online safety advice to keep the children and staff safe • Approve and review the effectiveness of the Online Safety and Data Security Policy • Delegate a governor to act as online safety link • Online safety Governor works with the Online Safety Coordinator to carry out regular monitoring (including online safety incident logs, filtering etc) and report to Governors
Head Teacher and Senior Leaders	• To take overall responsibility for online safety provision • To take overall responsibility for data and data security • Ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. HfL • Ensure that all staff receive suitable CPD to carry out their online safety roles, and to train other colleagues, as relevant • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive online safety curriculum in place • Ensure that there is a system in place for monitoring online safety • Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil • Inform the local authority about any serious online safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review online safety with the school's technical support
Online Safety Coordinator	• Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of online safety policies and document • Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Lead and monitor a progressive online safety education that is embedded across the curriculum for pupils • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA online safety staff and technical staff • 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 • Meet with Senior Leadership Team and online safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator
Computing Subject Leader	• Lead and monitor a progressive online safety education that is embedded across the curriculum for pupils • Lead and monitor the delivery of the online safety element of the Computing curriculum • Ensure that the school website is adequately protected • Monitor and update online safety information on the school website for parents and pupils

Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUA • Act in accordance with the AUA and Online Safety and Data Security Policy • Report any suspected misuse or concerns to the Online Safety Coordinator and check this has been recorded • Provide appropriate online safety learning opportunities as part of a progressive online safety curriculum • Model the safe use of technology • Monitor Computing activity in lessons, extracurricular and extended school activities • Ensure pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • Be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand and sign the Pupil AUA, after discussing it with their parents/carers • Participate in online safety activities, follow the AUA and report concerns for themselves or others • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Understand that the Online Safety Policy covers actions out of school that are related to their membership of the school • Have a good understanding of research skills and the need to avoid plagiarism ad uphold copyright regulations
Parents and Carers	• Endorse (by signature) the Pupil AUA • Discuss online safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet • Access the school website in accordance with the relevant school AUA • Keep up to date with online safety information/issues through the school website, newsletters and other opportunities • Inform the Headteacher of any online safety issues that relate to the school, including their children's use of technology • Maintain responsible standards when using social media to discuss school issues, in accordance with the Social Media AUA
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, in which passwords are regularly changed • Maintain and inform the online safety coordinator of online safety issues, including relating to filtering • Keep up to date with online safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Coordinator for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUA detailing their extra responsibilities
Community Users (Visitors)	• On signing the Visitor book, visitors are made aware of their agreement to follow the Occasional Visitor's AUA and Code of Conduct before being provided with access to school systems

Online Safety in the Curriculum

Education of pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to e-safety'

School Inspection Handbook - Ofsted 2014

Computing and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum in which a progressive planned online safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Within this:

- key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons, including the display of the Smile and stay safe poster (see Appendix 2) in all classrooms and key public areas
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies when opportunities arise and as part of the online safety curriculum
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches
- pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information
- pupils are aware of 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, modelling and appropriate activities
- pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology
- pupils will read and sign an AUA at the beginning of each school year, which will be shared with parents and carers

- pupils are reminded of the Smile and stay safe

- pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button

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

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

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUA guidance which they are asked to sign with their children and regular newsletter and website updates;

- raising awareness through activities planned by staff and pupils;

- inviting parents to attend activities such as Safer Internet Day, online safety week, online safety assemblies or other meetings as appropriate;

- providing and maintaining links to up to date information on the school website

Online Safety Skills Development for Staff and Governors

There is a planned programme of online safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUAs.

- this Online Safety and Data Security Policy and its updates being shared and discussed in staff meetings and in Governor meetings

- an annual audit of the online safety training needs of **all** staff

- the online safety coordinator receiving regular updates through attendance at HfL and LA training sessions and by reviewing regular online safety newsletters from the LA
- staff are given opportunities to update their online safety knowledge and skills through training, guidance and direction to relevant newsletters, websites and other online resources
- the online safety coordinator providing guidance and training as required to individuals and seeking LA support on issues
- all staff are encouraged to incorporate online safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern
- new staff receive information on the school's AUA as part of their induction
- providing information to supply and student teachers on the school's online safety procedures
- all staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community (see online safety coordinator)
- staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772

Managing the School online safety messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used
- The online safety policy will be introduced to the pupils at the start of each school year
- Online safety posters will be prominently displayed
- The key online safety advice will be promoted widely through school displays, newsletters, class activities and so on
- We will participate in Safer Internet Day every February

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying

e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111.

Pupils, staff and parents/carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.

All incidents of cyberbullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of cyberbullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
- Internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUA
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Anti-Radicalisation and Counter-Extremism

Staff will sign a register to show that they have read and fully understand their responsibilities regarding The Prevent Duty document (June 2015). They have also be directed to read 'How Social Media is used to encourage travel to Syria and Iraq' document (see web link below).

'It is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified.' (pg5)

'…schools and childcare providers should be aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet.' (pg6)

'Schools and childcare providers should have clear procedures in place for protecting children at risk of radicalisation. These procedures may be set out in existing safeguarding policies.' (pg6)

'IT policies….

…the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

…schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum…..

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.' (pg8)

The Prevent Duty: Departmental advice for schools and childcare providers June 2015

For more information refer to the Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

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

Infrastructure

Lodge Farm 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

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's Acceptable Use Agreement in addition to the staff AUA.

The School ensures, when working with our technical support provider that the following guidelines are adhered to:

- We use the Hertfordshire Local Authority 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
- The School ICT systems are managed in ways that ensure that the school meets online safety technical requirements
- Appropriate security measures are in place to protect the serves, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school data
- It is the responsibility of the school, by delegation to the IT technician, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- If there are any issues related to viruses or anti-virus software, the IT technician should be informed via email or the communication book kept in the main reception office
- There are regular reviews and audits of the safety and security of school ICT systems
- 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 online safety coordinator or teacher as appropriate
- 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 or the IT technician's responsibility 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 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 the IT technician or Headteacher

- Access to the school network and Internet will be controlled with regard to:

  - Users having clearly defined access rights to school ICT systems through group policies

  - Users, from Year 2, are provided with a username and unique password

  - Staff users are aware that they are responsible for the security of their username and password which they are required to change termly. They must not allow other users to access the systems using their log on details

  - The 'master/administrator' passwords are available to the Headteacher and kept in the school safe

  - Users must immediately report any suspicion or evidence that there has been a breach of security

  - An agreed process being in place for the provision of temporary access of 'guest/visitors' (e.g. trainee or supply teachers) onto the school system. All 'guests/visitors', once they have signed the visitor book, agree to and will follow the 'Occasional Visitor's AUA and Code of Conduct', which is available in the school office (see Appendix 1).

  - Pupils will use age appropriate search engines and online tools and activities

Data Security and Protection

The accessing and appropriate use of school data is something that the school takes very seriously. This Online Safety and Data Security Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The Local Authority guidance documents listed below will support the school in how to keep data secure. HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

Also available are guidance documents on the SITSS website concerning 'Safe Handling of Data' (available on the grid at http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)

To ensure the security of its data, Lodge Farm Primary School will:

- direct staff to the guidance documents and weblinks above
- at all times take care to ensure the safe keeping of personal, sensitive, confidential or classified data, minimising the risk of its loss or misuse
- give relevant staff access to its Management Information System, with a unique username and password which it is their responsibility to keep secure
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- store or transfer data using approved services such as encryption and secure password protected devices
- make sure data is deleted from the device once it has been transferred or its use is complete
- 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

Protective Marking of Official Information

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

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

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

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. The Headteacher has the following responsibilities:

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

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

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 Headteacher, Co-headteacher and Finance and Office Manager should be 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, they are able to manage and address risks to the information and make sure that information handling complies with legal requirements. However, it should be clear to all staff 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.

Personal or Confidential Information

Protecting Personal or Confidential Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure 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 or confidential information you disclose or share with others
- Ensure that personal or confidential information is not disclosed to any unauthorised person
- Ensure the security of any personal or confidential information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal or confidential information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal or confidential information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal or Confidential Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- 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

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data. At the moment, SITSS do not encrypt servers, however Office PCs (including Office Master PCs) installed by SITSS are supplied with encryption software installed

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.

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance on *How to Encrypt Files* which contains guidance on creating strong passwords and password security
http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child or colleague your password
- If you aware of a breach of security with your password or account inform the online safety coordinator or IT technician immediately
- Passwords must be strong and be difficult to guess. They should contain a minimum of six characters which are a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 2 weeks

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

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 private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety and Data Security policy
- Users are provided with an individual network, email and Management Information System log-in username. From Year 2 they are also expected to use a personal

password and keep it private

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

- 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 termly. 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 10 minutes.

- In our school, all ICT password policies are the responsibility of the online safety coordinator and the IT technician. 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 unauthorised access

- Regularly change generic passwords to avoid unauthorised access

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 homework, 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

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- 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.

School website

- The Headteacher, in liaison with the Computing subject leader and online safety coordinator takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Uploading of information to the website is restricted to the Computing subject leader, online safety coordinator and the website manager.

- Uploading of information to class pages is the responsibility of the class teacher.

- The school website complies with the statutory DfE guidelines for publications

- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identify and status

- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;

- Photographs published on the web do not have full names attached;

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

- We do not use embedded geodata in respect of stored images

- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

e-mail

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

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

Managing e-mail

- The school gives all staff and governors 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
- Staff and governors should use their school email for all professional communication
- 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 emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- Staff must inform the online safety co-ordinator or Headteacher if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the Computing Programme of Study
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- The House and Vice Captains have their own school issued 'House' accounts. All other children use a class/ group e-mail address
- The forwarding of chain emails is not permitted in school.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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 or upsetting e-mail
- However you access your school e-mail, (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section ***emailing Personal or Confidential information*** below
- 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

Receiving e-mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; consult the IT technician first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal or Confidential Information

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

Either:
Obtain express consent from your Headteacher to provide the information by e-mail.

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

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

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

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

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. With regards to the following, **Lodge Farm Primary School** will:

Social media (including YouTube, Facebook, Twitter, blogging and personal publishing)

- not permit staff to use their personal social media accounts using school equipment
- endeavour to deny access to social networking and online games websites to pupils within school
- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
- encourage staff may only create blogs, wikis or other online areas in order to communicate with pupils and share learning using the school website or other systems approved by the Headteacher
- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- ensure that any digital communication between staff and pupils or parents and carers is always professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards 2012
- advise staff that no reference should be made to pupils, parents/carers or school staff
- advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- register concerns (e.g. recording in online safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them online

- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team

- advise all pupils to be cautious about the information given by others on such websites, for example users not being who they say they are

- teach pupils 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

- remind pupils 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)

- advise pupils to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- encourage pupils to be wary about publishing specific and detailed private thoughts and information online

- ask pupils to report any incidents of Cyberbullying to the school

- when signing up to online services that require the uploading of what could be deemed as **personal or sensitive data**, Lodge Farm will check terms and conditions regarding the location of storage. Please see the Safe Harbor Agreement Statement http://www.thegrid.org.uk/info/dataprotection/#data

  Also: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/

- remind parents/carers and pupils that services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

- regularly provide staff, governors, pupils, parents and carers with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- ensure 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

- ensure staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Mobile phones

- allow 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

- does not allow staff to use personal electronic devices (including smart watches) in public areas of the school, except the staffroom, unless approved by the online safety coordinator or Headteacher, between the hours of 8.30am and 3.30pm.
- does not allow staff to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- allows this technology to be used for educational purposes, as mutually agreed with the Headteacher e.g. school visits. The device user, in this instance, must always ask the prior permission of the bill payer
- allows pupils in Year 6 to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent. If they have been given permission to bring their mobile phone to school, they will only use it at the end of the school day once they have left the school site
- informs visitors of the school's expectations regarding the use of mobile phones
- reminds staff that all personal devices should be password protected
- not be responsible for the loss, damage or theft of any personal mobile device
- does not allow the sending of inappropriate text messages between any member of the school community
- seeks permission before any image or sound recordings are made on these devices of any member of the school community
- makes users aware that when bringing personal devices into school they must ensure there is no inappropriate or illegal content on the device
- maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

Other personal devices

- allow pupils to bring their own device e.g. USB, to support planned learning experiences
- ensure pupils using their own device sign an addition to the pupil AUA to agree to responsible use
- makes staff aware that the staff AUA they sign will apply to staff using their own portable device for school purposes
- enable and insist on the use of the school's Internet connection while on the school site
- inform all that personal devices should be charged prior to bringing it to school

- maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

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 HCC and school policies.

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

- 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 your incoming telephone calls can be handled at all times

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. HCC guidance can be found:
http://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. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication
- All parties must recognise that any published image could be reused and repurposed

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

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

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

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

Parents or carers may withdraw permission, in writing, at any time. 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 online safety coordinator or the Headteacher has 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 (eg, 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
- When a pupil has left the school or images are no longer required, images are deleted.

Webcams and CCTV

- The school uses CCTV for security and safety. 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)
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- 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

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is 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

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety 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 online safety policy though parent forums, invitation to Internet Safer week, pupil voice and school council
- Parents/carers are asked to read through and sign acceptable use agreements on along with their child on admission to the school and then at the start of every academic year
- 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 (eg, on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement(s)
    - → **I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.**
    - → **I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.**
    - → **I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).**
    - → **I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.**
- The school disseminates information to parents relating to online safety where appropriate in the form of;
    - Information evenings
    - Practical training sessions eg current online safety issues
    - Invitation to Safer Internet Day
    - Posters
    - School website information
    - Newsletter items

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

School ICT Equipment

- As a user of the school ICTequipment, you are responsible for your activity
- 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. 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 Bursar. 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 Bursar. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

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

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. 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

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 for their identification badge and contact their department. 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 Data Protection Act 1998, 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 Data Protection Act 1998, 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.

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider (eg Herts for Learning Ltd).

Breaches

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

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

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

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

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

For pupils, online safety breaches will be dealt with in accordance with our behaviour policy.

Reporting and Response to incidents

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owners (IAOs), who are the Headteacher, Co-headteacher and the Bursar.

The school will follow Hertfordshire's *How to manage an online safety incident* by referring to the three flowcharts developed by the HSBC eSafety subgroup and which can be downloaded at http://www.thegrid.org.uk/eservices/safety/incident.shtml, (see Appendix 3), to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of Child abuse then the monitoring will be halted and referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content). The breach must be immediately reported to the online safety coordinator or Headteacher
- 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 and online safety coordinator. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- The online safety coordinator and/or Headteacher will record all reported incidents and actions taken in the School online safety incident log (see Appendix 4) and in any other relevant areas e.g. Bullying or Child Protection log
- The designated Child Protection Coordinator will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage pupil online safety incidents in accordance with the School Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Hertfordshire Children Safeguarding Team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior Education Technology Adviser

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

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
- Ensure you remove portable media from your computer when it is left unattended
- 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, 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.

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

  Data Protection Act 1998
  https://ico.org.uk/for-organisations/education/
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

- The school's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    i) verification of software licensing
    ii) any personal data likely to be held on the storage media? *
  - How it was disposed of eg waste, gift, sale
  - Name of person and/or organisation who received the disposed item

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

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

Further information available at:
Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

https://ico.org.uk/

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

https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information

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

Further help and support

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

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

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

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

Test your online safety skills http://www.getsafeonline.org

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

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

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 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

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 online safety

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.

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 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 a 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

Safe Harbor Agreement Statement
http://www.thegrid.org.uk/info/dataprotection/#data

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/

The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance
https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

Appendixes

Appendix 1: Acceptable Use Agreements

Staff, Governors and Visitors Acceptable Use Agreement and Code of Conduct

IT Technician Acceptable Use Agreement

Professional Responsibilities

EYFS and KS1 Pupil Acceptable Use Agreement and Online Safety Rules

KS2 Pupil Acceptable Use Agreement and Online Safety Rules

Parent/Carer Social Media Acceptable Use Agreement

Occasional Visitors Acceptable Use Agreement and Code of Conduct

Appendix 2: Smile and stay safe poster

Appendix 3: How to manage an online safety incident - three flowcharts

Appendix 4: School online safety incident log