WESTON HILLS CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY AND DATA SECURITY POLICY FOR ICT ACCEPTABLE USE

Review date: Spring 2017

CONTENTS

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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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. At Weston Hills, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviour 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.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling are aware of the risks and threats and how to minimise them. Both this policy and the Acceptable Use Agreement (for staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, etc).

ESAFETY

eSafety – Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school. The Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Mrs. S. Alexander who has been designated this role. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Lincolnshire LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. The Governors and Headteacher are updated by the eSafety co-ordinator and have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health & safety, home-school agreements and behavioural/pupil discipline policies and PSHE.

eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in both ICT and PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities
- Pupils are aware of the impact of Cyber bullying 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 Childline
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

SMILE AND STAY SAFE

eSafety guideline which are displayed throughout the school

- Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.
- Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.
- Information online can be untrue. Someone online may not be telling the truth about who they are – they may not be a 'friend'.
- Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.
- Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message – so do not open or reply.

eSafety Skills Development for Staff

- Our staff receive information and training on eSafety issues in the form of staff meetings, training days and hard copies for information.
- 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.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the School eSafety Messages

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

EQUAL OPPORTUNITIES

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn aids 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.

PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school. We inform parents/carers and seek to promote a wide understanding of the benefits related to ICT, eSafety 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).
- The school disseminates information to parents relating to eSafety where appropriate in the form of posters, website and newsletter items.

PUPIL ACCEPTABLE USE POLICY FOR INTERNET AND E-MAIL

Weston Hills C of E Primary School operates the following policy on use of the internet by pupils at the school:

1. Pupils must obtain the permission of parent(s) / guardian(s) before they can be allowed to use the Internet or education E-mail service. The Parental Permission Form must be signed and returned to school.
2. Pupils should only use the school computer systems for those activities and services (Internet and E-mail) which they have been given permission to use.
3. Pupils must only use the school computers with the permission of a member of staff.
4. Activities which use the Internet during taught lessons will be directly related to school work. Use of the Internet outside of taught lessons is at the discretion of a member of staff who will set guidelines and rules for its use.
5. The internet is not to be used to access anything which is illegal or anything that someone else may find offensive. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know.
6. Pupils must only use the user name and password that they have been given, do not allow anyone else to use your details.
7. Social networking is not allowed in school.
8. Pupils should not download and use material or copy and paste content which is copyright.
9. The Internet access is filtered to stop access to unsuitable material. As no filtering system can be 100% effective, it is important that parents are aware that users of the system are required to act responsibly. Under no circumstances should pupils attempt to view, upload or download any material that is likely to be unsuitable for children or schools. Pupils have a responsibility to inform the member of staff supervising them if they have accidentally accessed inappropriate content.

10. Pupils will be taught to respect the privacy of files of other users. They will be taught not to enter, or attempt to enter without permission, the file areas of other pupils or staff.
11. Parents are asked to explain the importance to their child of these rules for the safe use of the Internet and to sign and return to the school the Parental Permission Form. No disks from home can be used on systems in school unless they have been virus scanned.
12. It is the policy of the school not to identify individual children in photographs used in local newspapers or on the Internet, unless parental permission is granted. For pictures used on web sites any images used are of groups of pupils.
13. You should never try to bypass any of the security in place; this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.
14. Mobile telephones should not be in school, if you need to bring a telephone into school for after school, then it must be handed into the school office until the end of the school day.

Parent's Statement

As a parent/guardian of ………………………………………. I acknowledge that I have read the Acceptable Use Policy on student use of the Internet and have discussed it with my child. I understand that this access is designed for educational purposes. I recognise that, whilst every effort will be made to monitor student use of the Internet, it is impossible for Weston Hills Church of England Primary School to continually monitor and restrict access to all controversial materials. I further acknowledge that, whilst questionable materials exist on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold the staff, head teacher or governors of Weston Hills Church of England Primary School responsible for any such materials acquired from the Internet.

My child may/may not use the Internet as part of their school studies.
(Please delete as appropriate).

Signed ……………………………………………. Date ……………………….

Parent/Guardian of ……………………………………………

Class …………………………………………..

ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS

Acceptable Use Agreement/Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety co-ordinator.

- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher of Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's eSafety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ……………………………………………………….. Date …………………………………………

Full Name ……………………………………………………………………………………… (printed)

Job Title ……………………………………………………………………………………………………..

INTERNET ACCESS

The internet is an open communication available to all. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- Pupils have supervised access to internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are 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 illegal to copy of 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 or confidential information in any way that may compromise its intended restricted audience.
- Don't reveal names of colleagues, or any other confidential information acquired through your job on any social networking site or blog.
- Online gambling or gaming is not allowed.

Infrastructure

- Staff and pupils are aware that school based email and interned activity can be monitored and explored further if required.
- If staff of pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the eSafety co-ordinator or teacher as appropriate.
- It is the responsibility of the Network Management Company (F1) to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies.
- If there are any issues related to viruses or anti-virus software, the ICT co-ordinator / F1 should be notified as soon as possible.

MANAGING OTHER WEB TECHNOLOGIES

At present the school denies access to social networking sites to pupils within school. Out of school thought the use of social networking sites is on the rise so our children need to be aware how to use them minimizing their risk.

- 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 not place images of themselves on such sites. This includes photographs which may provide location or identification information
- 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, 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 cyber bullying to the school

EMAIL

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’.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils is advised to cc. the Headteacher, when appropriate
- 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 you e-mail account as follows:

  - delete all e-mails of short-term value

- organise e-mails into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain letters is not permitted in school
- All pupil e-mail users are expected to adhere to the generally accepted 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
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail
- Staff must inform the eSafety Co-ordinator if they receive an offensive e-mail
- However you access your school e-mail (whether directly, through webmail when away from the school or on non-school hardware) all the schools e-mail policies apply
- The use of Hotmail, BT Internet, AOL or any other internet based webmail service for sending, reading or receiving business related e-mail is not permitted

Sending e-Mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Do not send or forward attachments unnecessarily. Whenever possible, send links or 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
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate folder

Future Developments

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in PROTECT – PERSONAL on the first line of the e-mail. This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, forms, including paper documents you send in hardcopy, etc). the name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

SAFE USE OF IMAGES

Taking of Images and Film

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, 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 pupil's device

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 website and/or 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.

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, except in the case of newspaper publication, which is insisted upon by the newspaper themselves.

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 Web Manage has authority to upload to this site.

Storage of Images

- Images of children are stored on the school's network and individual laptops accessible by password
- 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
- Members of the teaching staff have the responsibility of deleting the images when they are no longer required, or the pupil has left the school

COMPUTER VIRUSES

- All files downloaded from the internet, received via e-mail or on removable media (e.g. external drive, CD) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through F1
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment immediately and contact a member of the ICT team

SECURITY

- The school gives relevant staff access to its Management Information System (MIS), with a unique ID and password
- It is the responsibility of these staff to keep passwords secure
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keeps all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- It is the responsibility of individual staff to ensure the security of any personal, sensitive and confidential information contained in documents faxed, copied, scanned or printed

The SIRO (Senior Information Risk Owner) in this school is Mrs Jane Fitzgerald.

The SIRO is a senior member of staff who is familiar with information risks and the school's response. The SIRO has the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owner (IAO)
- They act as an advocate for information risk management

The IAO (Information Asset Owner) in this school is Mrs Heather Pocklington

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. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) is identified as an asset and has an Information Asset Owner. In example the MIS Administrator/Manager is the IAO.

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 of

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.

MONITORING

The ICT Team 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 contact the ICT co-ordinator. The ICT co-ordinator 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.

ICT authorised staff, may monitor, record and disclose telephone calls, e-mails, internet use and any other electronic communications involving its employees, without consent, to the extent permitted by law. This may be to confirm school business related information, to investigate compliance with school policies, standards and procedures, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime. All monitoring, surveillance or investigate 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.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the eSafety co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to a member of the ICT team.

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- 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. If the storage media has failed it will be physically destroyed.
- Disposal of any ICT equipment will conform to: 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/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 maintains a comprehensive inventory of all its ICT equipment, including a record of disposal.

INCIDENT REPORTING, eSAFETY INCIDENT LOG & INFRINGEMENTS

Incident Reporting

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

eSafety Incident Log

Weston Hills Church of England Primary School eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety co-ordinator. This incident log is monitored termly by the Headteacher or Chair of Governors.

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

Misuse and Infringements

Complaints and/or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents are logged and the **Flowcharts for Managing an eSafety Incident** are followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence

PASSWORDS AND PASSWORD SECURITY

Passwords

- Always use your own personal password to access computers
- Make sure you enter your personal password each time you logon. Do not include password in any automated logon procedures

- Staff should change temporary passwords at first logon via the computer suite
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system

Password Security

Password security is essential for staff, particularly if they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff and pupils are regularly reminded of the need for password security.

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

Zombie Accounts

Zombie accounts refer 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. All user accounts are disabled once the member of the school has left.

PERSONAL INFORMATION PROMISE

The Information Commissioner's Office launched a Personal Information Promise in January 2009. Schools may wish to sign up to this promise which is shown below.

The Personal Information Promise is:

I, Mrs Jane Fitzgerald, on behalf of Weston Hills Church of England Primary School, promise that we will:

1. Value the personal information entrusted to us and make sure we respect that trust;
2. Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. Be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;

7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises;
10. regularly check that we are living up to our promises and report on how we are doing.

PERSONAL OR SENSITIVE INFORMATION

Protecting Personal, Sensitive or Confidential 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 or confidential information you disclose or share with other
- Ensure that personal, sensitive or confidential information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive or confidential information contained in documents you fax, copy, scan or print
- Only download personal data from systems if expressly authorised to do so by the Headteacher
- You must not post on the internet personal, sensitive 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, sensitive or confidential information
- Ensure hard copies of data are securely stored and disposed of after use

Storing/Transferring Personal, Sensitive 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

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 access information such as logon IDs confidential and do not disclose them to anyone
- 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

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
- The school logs ICT equipment issued to staff and records 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
- 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 laptops
- 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, return all ICT equipment to the ICT co-ordinator. 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 or confidential information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the ICT co-ordinator who is responsible for:

    - Maintaining control of the allocation and transfer of equipment
    - 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 and removable data storage devices.

- 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.
- 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 Team, fully licensed and only carried out by your ICT Co-ordinator
- 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

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device
- In general pupils are discouraged from bringing personal mobile devices/phones to school unless the class teacher has written permission from parent or carer. In this instance the mobile device/phone is to be stored with the Class Teacher during teaching time. They should be switched off at all times.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

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

- Where the school provides mobile technologies such as phones and laptops for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

SERVERS

- Always keep servers in a locked and secure environment
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data on backup tapes must be backed up regularly and must be securely stored in a fireproof container
- Remote back ups should be automatically securely encrypted by Mouchel

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

MOBILE PHONES

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones

- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

WRITING AND REVIEWING THIS POLICY

Review Procedure

- There is an on-going opportunity for staff to discuss with the eSafety Co-ordinator any issue of eSafety that concerns them
- There is an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them
- This policy will be reviewed annually and consideration given to the implications for future whole school development planning
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way
- This policy has been read, amended and approved by the staff, head teacher and governors on 12th October 2012

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 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 anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 200

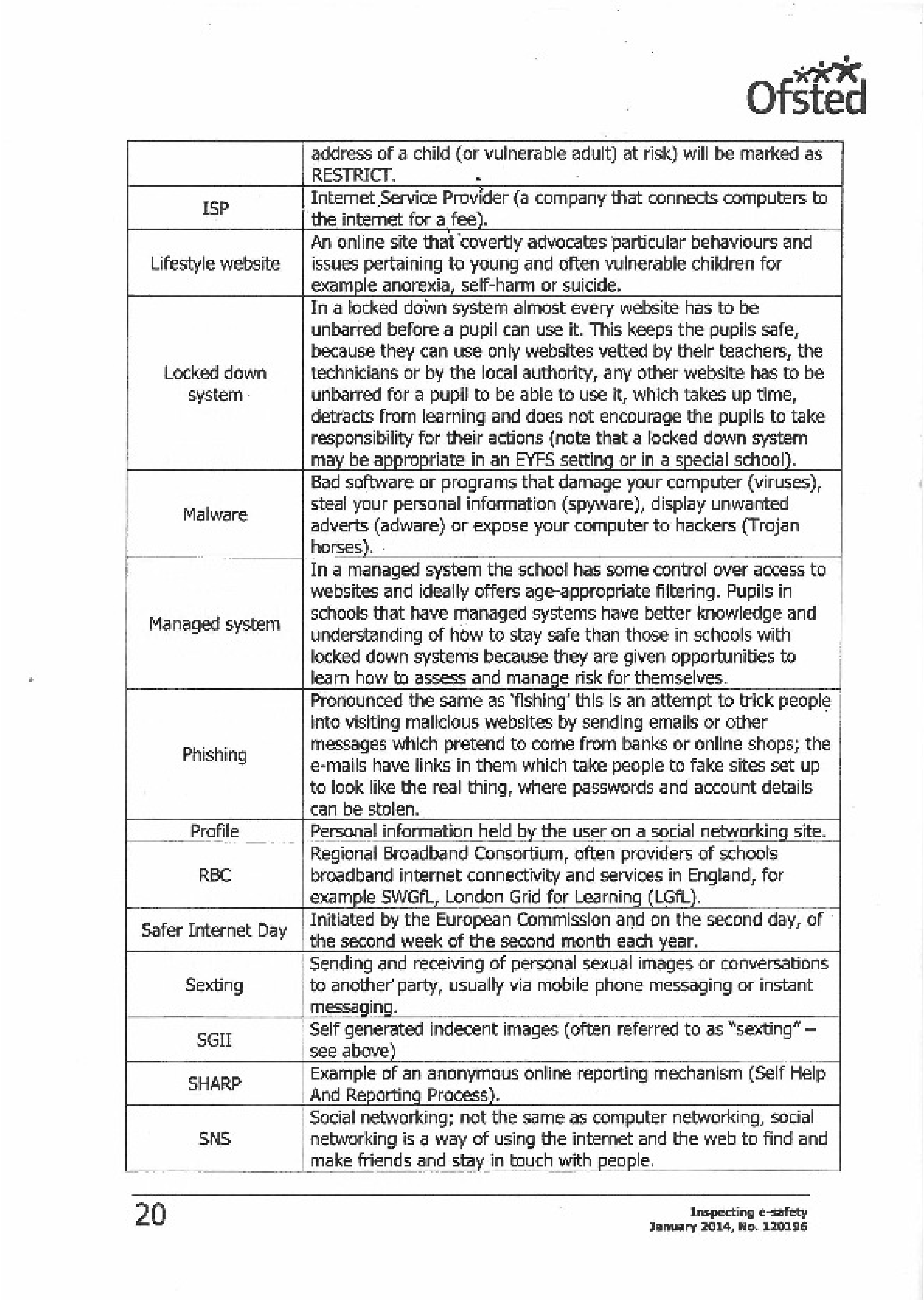
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Annex 6. Glossary

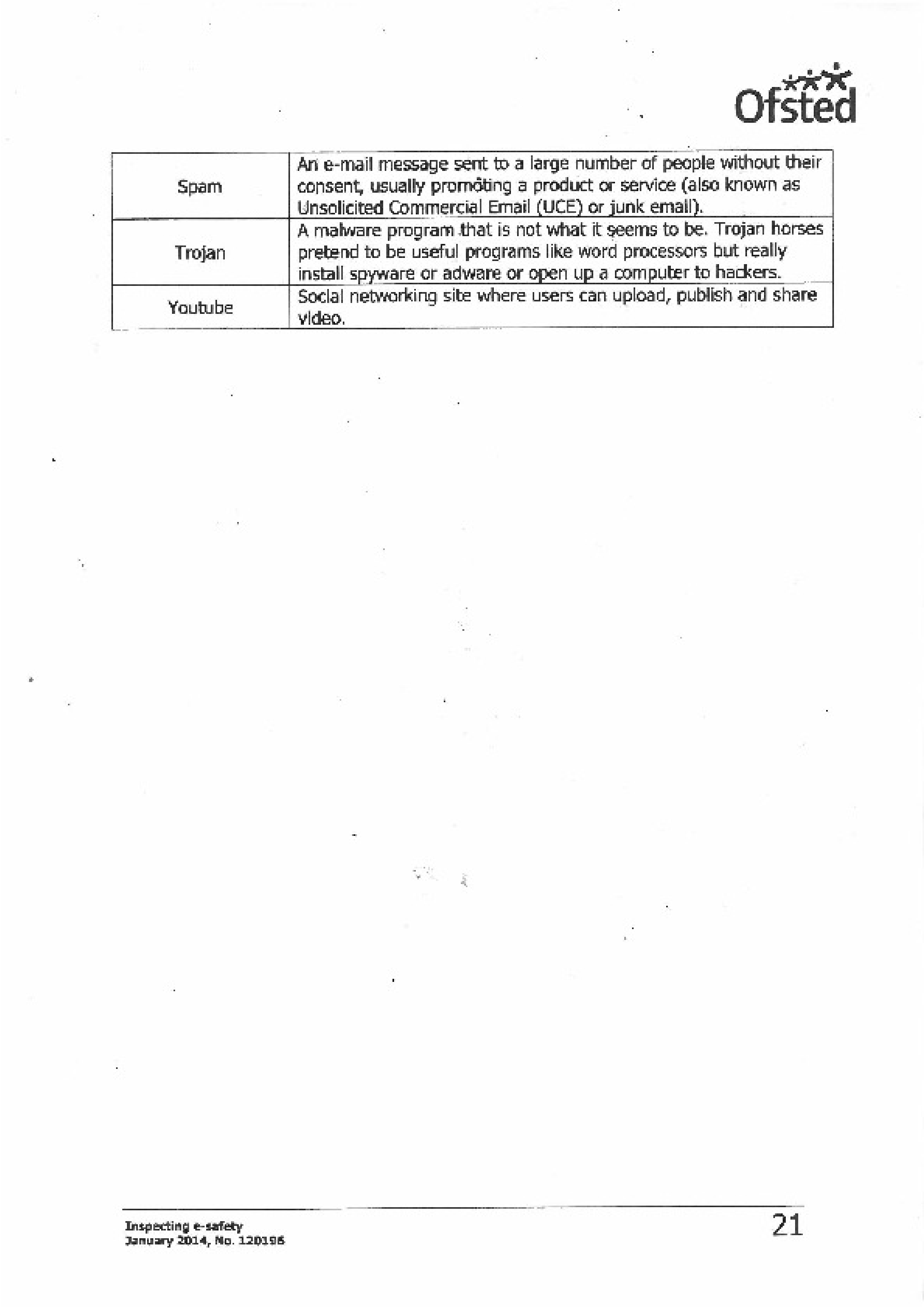
Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/.

In addition, the following terms used in this document are explained below

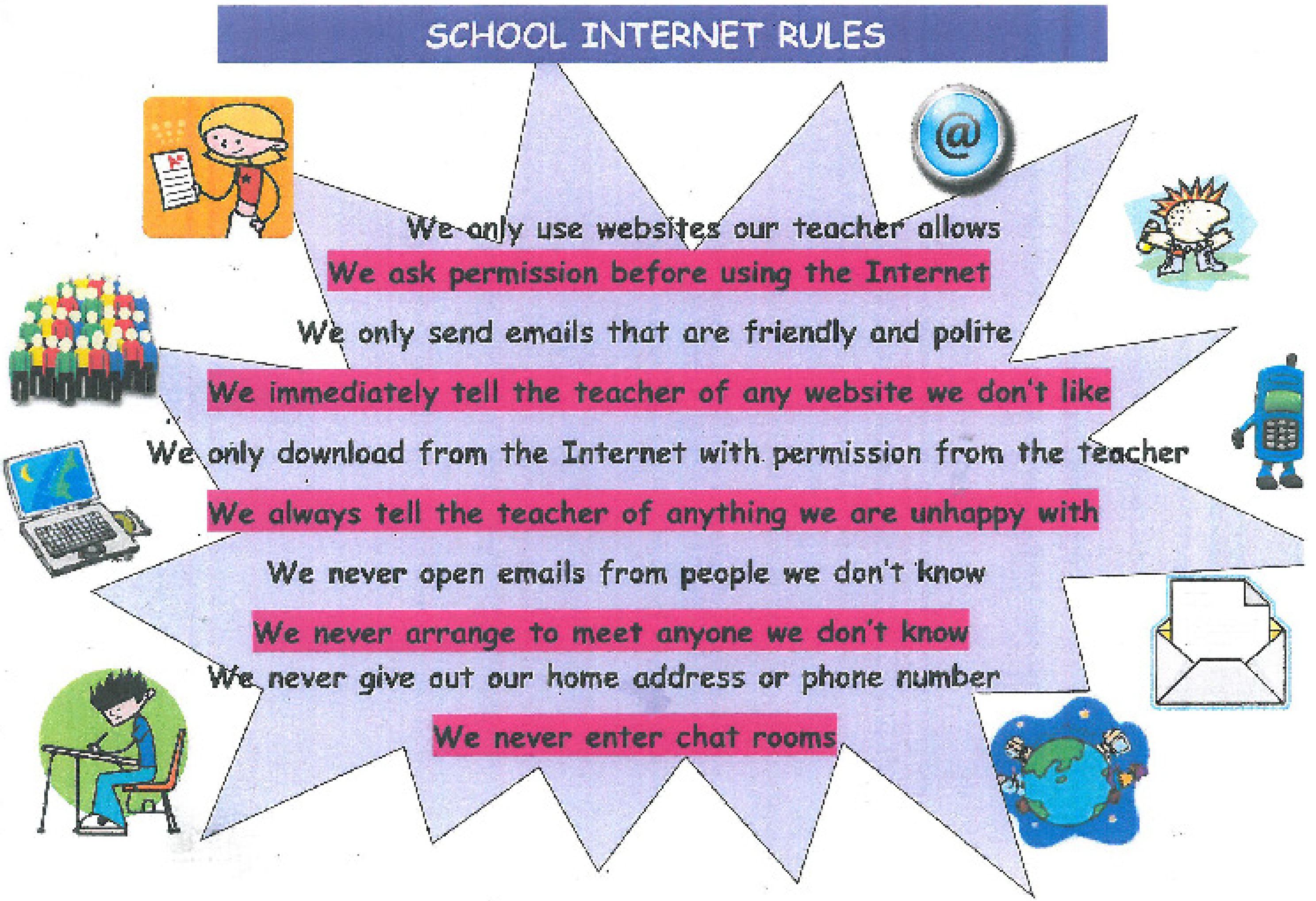
360 degree safe	SWGfL's online self-review tool for school improvement in online safety www.360safe.org.uk.
Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World' available at http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
EPICT	European Pedagogical ICT Accreditation.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
Impact level	Impact levels indicate the sensitivity of data and the associated protection required (see the government published HMG Security Policy Framework http://www.cabinetoffice.gov.uk/spf). The scheme uses five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification, however some (for example the home



	address of a child (or vulnerable adult) at risk) will be marked as RESTRICT.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self generated indecent images (often referred to as "sexting" – see above)
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.



Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
Youtube	Social networking site where users can upload, publish and share video.



SCHOOL INTERNET RULES

We only use websites our teacher allows

We ask permission before using the Internet

We only send emails that are friendly and polite

We immediately tell the teacher of any website we don't like

We only download from the Internet with permission from the teacher

We always tell the teacher of anything we are unhappy with

We never open emails from people we don't know

We never arrange to meet anyone we don't know

We never give out our home address or phone number

We never enter chat rooms