# Panshanger Primary School
# Policy for e-Safety and Acceptable Use of ICT

## Introduction

This policy contributes to pupil's safety, well-being, enjoyment and achievement within the context of the following school aims and the Every Child matters Agenda:

- To create a happy, caring and stimulating learning environment in which children can enjoy, achieve and thrive;
- To realise each child's full potential by promoting healthy lifestyles and by providing a wide range of learning opportunities for academic, social, emotional, moral, spiritual, cultural, and physical development.
- To provide a broad and balanced curriculum appropriate to the children's needs and in accordance with the early Learning Goals and the National Curriculum;
- To raise self esteem and confidence by helping each child to gain a sense of achievement and to take pride in that achievement.

The policy has been informed by advice and guidance from Herts for Learning and Hertfordshire Safeguarding Children Board

## Vision Statement

ICT is an integral part of everyday life and is seen as an essential resource to support learning and teaching. At Panshanger our vision is for ICT to be embedded across the school and for children to develop the skills to access life-long learning and employment in order to be well prepared to meet the future challenges of a changing world. They will be confident, well motivated and capable users of ICT with positive attitudes towards developing and changing technologies. ICT will enhance and extend children's learning opportunities across the curriculum and support personalisation of learning, high quality teaching, efficient management and administration and effective communication.

## Rationale for the Policy

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning and is constantly evolving. 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, usually 13 years.

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

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

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties 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 and pupils – see Appendices 1 and 2) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, tablets, mobile devices, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

**Monitoring**

All Internet activity is logged by the school's Internet provider. These logs may be monitored by authorised HCC staff.

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, reference will be made to the school's behaviour policy.

**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 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 the Head Teacher.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

**Computer Viruses**

- All files downloaded from the Internet, received via e-mail or on removable media, such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used.
- Staff must never interfere with any anti-virus software installed on school ICT equipment
- If a machine is not routinely connected to the school network, provision will be made for regular virus updates through the school's IT provider
- If a virus is suspected on any school ICT equipment, the equipment must not be used and the school's ICT support provider contacted immediately. The ICT support provider will advise what actions to take and be responsible for advising others that need to know

## Data Security

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

The Local Authority guidance documents are listed below

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

### Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

### Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents
- HCC recommend 3 levels of labelling
- Unclassified (or if unmarked) – this will imply that the document contains no sensitive or personal information and will be a public document
- Protect – this should be the default setting and be applied to documents containing

any sensitive or personal data. Marking documents as Protect will demonstrate an awareness of the Data Protection Act and the school's responsibilities

- Restricted – documents containing any ultra sensitive data for even one person should be marked as Restricted

---

**Relevant Responsible Persons**

Senior members of staff should be familiar with information risks and the school's response. Sometimes called a SIRO, there should be a member of the senior leadership team who 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.

---

**Information Asset Owner (IAO)**

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff 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 this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

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.

## 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:
  - verification of software licensing
  - any personal data likely to be held on the storage media? *
- How it was disposed of eg waste, gift, sale
- Name of person & / or organisation who received the disposed item

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

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

Further information 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

**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 are advised to cc. the Headteacher, line manager or designated line manager
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of 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
- Pupils do not have their own individual school issued accounts but use a class/ group e-mail address
- 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 without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the eSafety co-ordinator if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- 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.
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted.

**Sending e-Mails**

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section
- e-mailing Personal, Sensitive, Confidential or Classified **Information**
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)
- 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

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail
- School e-mail is not to be used for personal advertising

**Receiving e-Mails**

- E-mail should be checked regularly
- Activate your 'out-of-office' notification when away for extended periods
- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

**e-mailing Personal, Sensitive, Confidential or Classified Information**

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
  - Verify the details, including accurate e-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

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

- Hertfordshire Constabulary
- Hertfordshire Partnership Trust

**Future Developments**

There is currently a review taking place on the way e-mails are sent whereby all such communications are sent using GCSx. GCSx stands for the Government Connect Secure eXtranet. It provides a more secure communications system (i.e. more secure than the internet).

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. *Not sure staff are aware of this*

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.

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

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

**eSafety - Roles and Responsibilities**
As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Sarah Holt who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

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

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

- The school has a framework for teaching internet skills in ICT computing lessons
- 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 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 and respecting other people's information, images, etc through discussion, modeling and activities
- 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 Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT / computing curriculum.

**eSafety Skills Development for Staff**
- Our members of staff receive regular information and training on eSafety issues during staff meetings.
- Details of the ongoing staff training programme can be found on the Herts Grid for Learning.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas
- We will participate in Safer Internet Day every February.

**Managing the School eSafety Messages**
- We endeavour to embed eSafety messages across the curriculum whenever the Internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year eSafety posters will be prominently displayed

**Incident Reporting, eSafety Incident Log & Infringements**
**Incident Reporting**
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's 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 the Head Teacher. (See Appendix 3 for Incident Record Form).

**Misuse and Infringement**
**Complaints**
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed (See Appendix 4).

**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; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct during their induction.

**The INTERNET**

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Hertfordshire Grid for Learning (HGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

**Managing the Internet**

- The school maintains a list of pupils who will have supervised access to Internet resources (where reasonable) 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 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 its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

**Infrastructure**

Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded

School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to

http://www.thegrid.org.uk/eservices/safety/filtered.shtml

- Panshanger is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first. Pupils are discouraged from bringing in their own hardware e.g. memory sticks
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT / computing subject leader
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the ICT subject leader.

**Managing Other Web 2 Technologies**

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to pupils within school.
- Our pupils are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using systems approved by the Headteacher

**Parental Involvement**

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

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through consultation via school newsletters and with the School Council.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
  Parents/carers are expected to sign a Home School agreement containing the following statement: **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website
  - Newsletter items

**Passwords**

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include

passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff and pupils who have left the School are removed from the system within one month
- 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 secret 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 e-safety Policy and Data Security
- Users are provided with an individual network, email, and Management Information System (where appropriate) log-in username. From Year 3 children may be set up with personal passwords if appropriate.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is set by the school's ICT provider.
- In our school, all ICT password policies are the responsibility of Head Teacher and all staff and pupils are expected to comply with the policies at all times

**Taking Images**

- 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 solely to the school's network and deleted from the staff device as soon as practicable.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others. However with the express permission of the Headteacher, images can be taken provided they are transferred solely to the school's network and deleted from the pupil's device as soon as practicable.

**Consent of Adults Who Work at the School**

- Permission to use images of all staff who work at the school will be 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/ 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.

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 Manager has authority to upload to the site.

**STORAGE OF IMAGES**

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

**Web Cam and CCTV**

- The school does not use CCTV at present.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs / contacting Father Christmas in his grotto and never using images of children or adults
- 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)
- If webcams are used, notification will be given in the areas filmed by webcams by signage
- Consent will be sought from parents/carers and staff on joining the school, in the same way as for all images

**Video Conferencing**

- Permission will be sought from parents and carers if their children are to be involved in video conferences
- Permission will be sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils will be supervised by a member of staff when video conferencing
- All pupils will be supervised by a member of staff when video conferencing with end-points beyond the school
- The school will keep a record of video conferences, including date, time and participants.
- Approval from the Headteacher will be sought prior to all video conferences within school
- The school conferencing equipment will not be set to auto-answer and will only be switched on for scheduled and approved conferences
- No part of any video conference will be recorded in any medium without the written consent of those taking part

**School ICT Equipment**

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for: maintaining control of the allocation and transfer within their Unit and 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 and Mobile ICT Equipment**

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

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

**MOBILE TECHNOLOGIES**

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

**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
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. They should be stored in the office unless required in class for a specific purpose. At all times the device must be switched onto silent
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

**School Provided Mobile Devices (including phones)**

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

**Removable Media**

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please:

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

**Mobile Phones**

The school has one mobile 'pay-as-you-go' phone which is kept by the pool for use in emergencies or for pools supervisors to contact the pool carers / other supervisors. Security of the mobile phone is the responsibility of the pool supervisor on duty. Only school SIM cards must be used in school provided mobile phones; calls and texts to premium rate numbers and any numbers outside of the UK are not allowed. The school must be reimbursed for any personal calls made on the mobile phone.

The loss or theft of any school mobile phone equipment should be reported to the Head teacher immediately.

**Appendices**

**1 - Acceptable Use Agreement – Pupils**
**2 - Acceptable Use Agreement Staff and Governors and Professional Responsibilities –**
**3 - Incident Log**
**4 - Hertfordshire Flowcharts for Managing an eSafety Incident**
**5 – Smile and Stay Safe Poster**
**6 – Current Legislation**

*School Effectiveness Committee*
*June 2015*

**Panshanger Primary School**
**Acceptable Use of ICT Agreement / eSafety Rules**

Dear Parent/ Carer,

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

Please read and discuss these eSafety rules with your child and return one signed copy to the school. Thank you. If you have any concerns or would like some explanation please contact Mrs Holt.

**Parents**

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

- 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 approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I/we will support the school's policies on safeguarding and anti-bullying 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).

**Children**

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day.
- I will not sign up to online services until I am old enough to do so (13+ in most cases).

**Parent/ carer signature**

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

Parent/ Carer Signature ……

Class …… Date ……

(Please sign and return one copy and keep one copy for your records. Thank you.)

**Panshanger Primary School**
**Staff, Governor and Visitor**
**Acceptable Use of ICT 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 members of staff are aware of their professional responsibilities when using any form of ICT. All members of staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or Deputy Headteacher.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Computing Subject leader / Leverstock (IT provider)
- 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 understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will not wear a Smart Watch in public areas of the school premises.
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm except in the staff room.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- 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 . . . . . ..

*Reviewed and updated: September 2016*

## Staff Professional Responsibilities

The HSCB eSafety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions.


**Appendix 3**

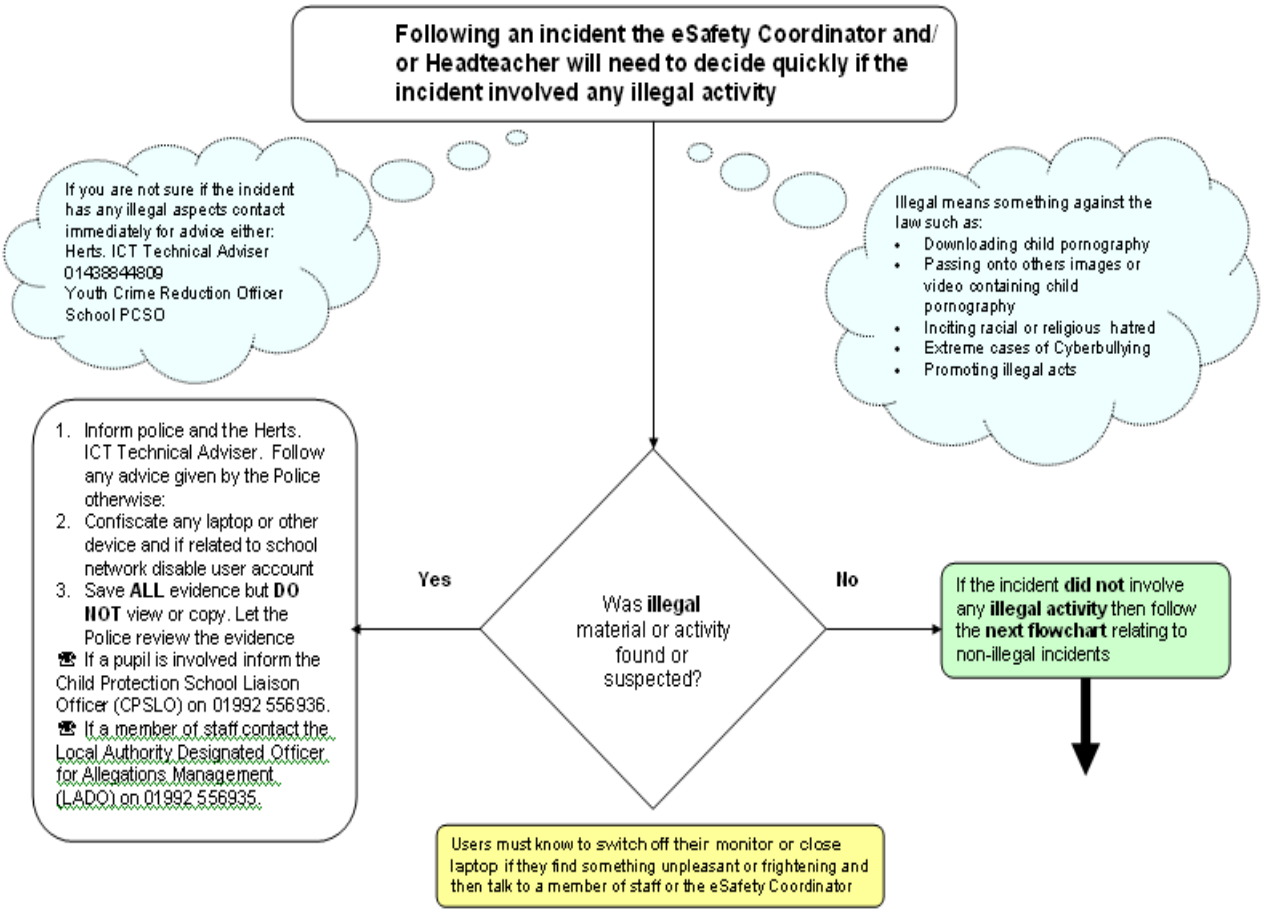
# Panshanger Primary School eSafety Incident Log

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

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

# Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident

## For Headteachers, Senior Leaders and eSafety Coordinators



## Smile and Stay Safe Posters

**eSafety guidelines to be displayed throughout the school**

# SMILE and stay safe

**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

**M**eeting 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.

**I**nformation online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

**L**et 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.

**E**mails, 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.

# Cyberbullying
# SMILE and stay safe

Staying safe and not being a victim of cyberbullying means keeping your personal details private, such as full name and phone number. Never let anyone know your password and try to choose hard to guess passwords that include numbers and symbols such as $.

Make sure you think before sending a text or image of yourself or someone else. Remember that once some information about you or others has been sent by text or posted on a social network, such as Facebook - it can be made public and may stay online for ever!

If you send messages to others remember to think about the impact of your words and images. If you receive a rude, nasty or unpleasant message or image about someone else do not forward as you could be helping the bully, or be accused of being the bully or even break the law.

Let a parent, carer, teacher, anti-bullying coordinator or trusted adult know if you are ever bullied. You can also call Childline on **0800 1111** in confidence.

Emails, text messages, chat rooms and social networks are some of the technologies that are used to cyberbully. These technologies will all contain evidence of any bullying and this evidence can be kept and used as proof of cyberbullying.

# Current Legislation

## Acts Relating to Monitoring of Staff eMail

### Data Protection Act 1998

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

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

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

### Regulation of Investigatory Powers Act 2000

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

### Human Rights Act 1998

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

## Other Acts Relating to eSafety

### Racial and Religious Hatred Act 2006

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

### Sexual Offences Act 2003

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

### Communications Act 2003 (section 127)

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

### The Computer Misuse Act 1990 (sections 1 – 3)

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

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

## Malicious Communications Act 1988 (section 1)

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

## Copyright, Design and Patents Act 1988

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

## Public Order Act 1986 (sections 17 – 29)

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

## Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is 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

## The Freedom of Information Act 200

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