**ROUND HILL ICT POLICY**

**&**

**INTERNET USE**

**&**

**E-SAFETY**

**CONTENTS**

Introduction 3

Monitoring 4

Incident Reporting 5

Computer Viruses 5

Security 5

Senior Information Risk Owner (SIRO) 6

Information Asset Owner (IAO) 6

Disposal of Redundant ICT Equipment 7

Managing E-Mail 8

Equal Opportunities 9

E-Safety 9

Misuse and Infringements 10

Inappropriate material 11

Managing the Internet 11

Parental Involvement 12

Password Security 12

Protecting Personal, Sensitive, Confidential and Classified Information 13

Publishing Work and Images 13

Storage of Images 14

School ICT Equipment 14

Personal Mobile Devices 14

Removable Media 14

Servers 15

Amendment – Pupil Mobile Phone Use 15

Current Legislation 16

Other Acts relating to E-Safety 17

**E-Safety Coordinator is Adrian Nash**

**Information Asset Owner is Isobel Greenhalgh.**

**Senior Information Risk Owner is Adrian Nash.**

**ROUND HILL ICT POLICY**

**including INTERNET USE and E-SAFETY**

**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 teach children in the use of these technologies in order to prepare them with the skills to access life-long learning and employment.

At ***Round Hill*** we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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. The internet technologies children are using both inside and outside of the classroom include:

* Websites
* Learning Platforms
* E-mail
* Texting
* Social Networking including chat rooms
* Blogs
* Podcasting
* 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.

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 should be made aware of the risks and threats and how to minimise them.

This policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) include any technologies provided by the school (such as PCs, laptops, webcams, interactive whiteboards, digital video and photo equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

**MONITORING**

All internet activity is logged by the school’s internet provider. Authorised ICT staff may inspect any ICT equipment owned by the School at any time. At Round Hill this will be the ICT coordinator, staff from System Education or the head teacher.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose any electronic communications involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain information under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

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

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

**INCIDENT REPORTING**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s ICT coordinator or e-Safety 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.

# COMPUTER VIRUSES

* All files downloaded from the Internet, received via e-mail or on removable media (e.g memory sticks, CDs) 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 that you use
* If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
* If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

**SECURITY**

* 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
* Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
* Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
* Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
* Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
* It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

**SENIOR INFORMATION RISK OWNER (SIRO)**

The SIRO is a senior member of staff who is familiar with information risks and the school’s response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

* they own the information risk policy and risk assessment
* they appoint the Information Asset Owner(s) (IAOs)
* they act as an advocate for information risk management

The Office of Public Sector Information publication Managing Information Risk provides further information.

The SIRO in this school is Adrian Nash. .

**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.

The IAO is Isobel Greenhalgh.

The role of an IAO is to understand:

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

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

However, 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

* All redundant ICT equipment will be disposed off 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 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 & Electronic Equipment Regulations 2006

The Waste Electrical & Electronic Equipment (Amendment) Regulations 2007

[www.environmentagency.gov.uk/business/topics/waste/32084.aspx](http://www.environmentagency.gov.uk/business/topics/waste/32084.aspx)

www.opsi.gov.uk/si/si2006/uksi\_20063289\_en.pdf

[www.opsi.gov.uk/si/si2007/pdf/uksi\_20073454\_en.pdf?lang=\_e](http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e)

 Data Protection Act 1998

[www.ico.gov.uk/what\_we\_cover/data\_protection.aspx](http://www.ico.gov.uk/what_we_cover/data_protection.aspx)

 Electricity at Work Regulations 1989

[www.opsi.gov.uk/si/si1989/Uksi\_19890635\_en\_1.htm](http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm)

* The school will maintain an 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:

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 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 website

# MANAGING E-MAIL

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

**STAFF**

* The school gives all staff their own e-mail account to use for all school business as a work based tool. **They are expected to check it daily.**
* It is the responsibility of each account holder to keep the password secure.
* **The school email account should be the account that is used for all school business.**
* All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
* 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 for archiving if needed
* Staff must inform (the e-Safety co-ordinator/line manager) if they receive an offensive e-mail.
* The use of an Internet based webmail service for sending, reading or receiving school related e-mail is not permitted.

**PUPILS**

* Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
* Children use a class/ group e-mail address
* 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.
* Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
* Pupils are introduced to e-mail as part of their learning using ICT.
* Never open attachments from an untrusted source; Consult your network manager first.

**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 Internet based webmail service for sending e-mail containing sensitive information is not permitted

**EQUAL OPPORTUNITIES**

The school endeavours to create a consistent message with parents for ALL pupils.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

**E-SAFETY**

As e-Safety 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 e-Safety co-ordinator in this school is Adrian Nash, 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 e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Notts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/e-Safety co-ordinator 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.

**E-SAFETY ACROSS THE CURRICULUM**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis.

We look for new opportunities to promote e-Safety across the curriculum.

• The school teaches internet skills including e-Safety and evaluating information when using ICT across the curriculum.

• They are taught that some rules are in place to protect them.

• Pupils are made aware of Cyberbullying and know how to seek help if they are affected by it. Pupils are made aware of where to seek advice or help if they experience problems when using the Internet.

**E-SAFETY AWARENESS FOR STAFF**

• Staff receive information and training on e-Safety issues during CPD sessions.

• 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 e-Safety and know what to do in the event of misuse of technology by any member of the school community.

• We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

• E-Safety posters are displayed around school.

. A CEOP link has been added to the new website (post Jan 2016) to enable parents and children to find guidance or report any inappropriate or worrying behaviour which they may experience whilst online.

**MISUSE AND INFRINGEMENTS**

Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher.

**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 e-Safety co-ordinator and 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.

**MANAGING 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. Whenever any inappropriate use is detected it will be followed up.

• Children have supervised access to Internet resources through the school’s fixed and mobile internet technology.

• Staff preview any recommended sites before use.

• 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 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.

• School internet access is controlled through the LA’s web filtering service.

• Round Hill is aware of its responsibility when monitoring staff communication under current legislation and will take 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.

• 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 (e.g. memory sticks) are responsible for measures to protect against viruses. It is not the school’s responsibility to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.

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

# PARENTAL INVOLVEMENT

We believe that parents/carers should involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities. There is a section on the school website with information for parents and games for children about e-Safety.

* 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 e-Safety where appropriate in the form of;
	+ Website postings
	+ Newsletter items
	+ Parents’ evenings

**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.

• Make sure you enter your personal passwords each time you logon.

• Change passwords whenever there is any indication of possible system or password compromise.

• Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else.

• Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks

• In our school, all ICT password policies are the responsibility of Adrain Nash and all staff and pupils are expected to comply with the policies at all times

**PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION**

* Ensure that any School information accessed from your own PC or removable media equipment is kept secure.
* Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
* Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
* Ensure hard copies of data are securely stored and disposed of after use.

**PUBLISHING WORK AND IMAGES**

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 local press

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.

**STORAGE OF IMAGES**

• Images/films of children are stored on the school’s network.

• Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

• Adrian Nash has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

**SCHOOL ICT EQUIPMENT**

• As a user of ICT, you are responsible for any activity undertaken on the school’s ICT equipment provided to you.

• ICT equipment issued to staff is recorded including serial numbers as part of the school’s inventory. All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for: maintaining control of the allocation, recovering and returning equipment when no longer needed.

• Staff must ensure that all ICT equipment that they use is kept physically secure.

• It is imperative that data is saved on a frequent basis to the school’s network drive. Personal or sensitive data should not be stored on the local drives of PCs.

• On termination of employment, resignation or transfer ICT equipment must be returned.

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

**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 not allowed to bring personal mobile phones to school.

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

**REMOVABLE MEDIA**

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section ‘**Error! Reference source not found.**’

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

# SERVERS

* Newly installed servers holding personal data should be encrypted, therefore password protecting data.
* Servers are in a locked and secure environment.
* Permissions are restricted using access policies.
* Servers are password protected.
* Data must be backed up regularly.

#

**POLICY ON THE USE OF MOBILE PHONES/ELECTRONIC EQUIPMENT**

This policy will be monitored, reviewed and amended as required by the head teacher and governors.  It should be read along with the policies listed below:

     Health and Safety

     Anti-bullying

     Chid Protection

     Internet Acceptable Use

Pupils are not permitted to bring mobile phones to school.
In **very exceptional** circumstances and when permission has been sought from the Head Teacher children may be able to bring a mobile phone into school under the following strict conditions:

     Proof is given that the child regularly walks home on their own

     A letter of permission is signed by the parent and given to the Head Teacher

     The phone is switched off and out of sight; and handed to the class teacher each day.

     The school accepts no liability for the loss/damage of any personal equipment while on school premises.

The use of mobile phones of Round Hill Primary School follows the guidance and direction given by the Local Authority:

     Round Hill Primary School actively discourages pupils from bringing mobile phones to school.

     Should parents/carers need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office, (Tel no 01159179262)

     Where a pupil is found by a member of staff to be using a mobile phone, the phone will be taken from the pupil, handed to a senior member of staff who will record the name of the child and attach to the phone. The mobile phone will be stored by that teacher. The pupil may collect the phone at the end of the school day. The right to bring mobile phones onto school premises will be revoked if a pupil fails to adhere to school policy.

     If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken according to the school’s discipline Policy.

     If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by the pupil in the presence of a teacher.

In addition mobile phones/recording equipment are not be used by pupils during educational visits for:

     Any form of communication with an individual.

     This includes phone calls/texts to parents/guardians. In the event that a pupil needs to contact home this will be arranged through the school office and teachers who are on duty.

Adrian Nash
Updated January 2011

# CURRENT LEGISLATION

# Acts Relating to Monitoring of Staff e-Mail

### Data Protection Act 1998 (amendments 2003)

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 E-SAFETY**

The following pieces of legislation can be viewed fro further advice if needed.

### 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](http://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) (Updated with effect from 30.10.16)

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.