



**eSafety**

**and**

**Data Security**

**Including Policies for ICT Acceptable Use**

# CONTENTS

INTRODUCTION.....	1
MONITORING.....	3
BREACHES .....	4
Incident Reporting.....	4
ACCEPTABLE USE AGREEMENT: STUDENTS - SECONDARY .....	5
ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS.....	11
STAFF PROFESSIONAL RESPONSIBILITIES.....	13
COMPUTER VIRUSES .....	14
DATA SECURITY .....	15
Security .....	15
Protective Marking.....	15
Relevant Responsible Persons.....	16
Information Asset Owner (IAO).....	16
DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY.....	17
E-MAIL.....	19
Managing e-Mail.....	19
Sending e-Mails.....	20
Receiving e-Mails .....	20
e-mailing Personal, Sensitive, Confidential or Classified Information .....	18
EQUAL OPPORTUNITIES.....	19
Students with Additional Needs .....	19
ESAFETY.....	23
eSafety - Roles and Responsibilities.....	23
eSafety in the Curriculum.....	23
eSafety Skills Development for Staff.....	24
Managing the School eSafety Messages .....	24
INCIDENT REPORTING, ESAFETY INCIDENT LOG & INFRINGEMENTS.....	25
Incident Reporting.....	25
eSafety Incident Log.....	25
Misuse and Infringements.....	25
Flowcharts for Managing an eSafety Incident .....	25
INTERNET ACCESS.....	29
Managing the Internet.....	29
Internet Use.....	29
Infrastructure.....	Error! Bookmark not defined.
MANAGING OTHER ONLINE TECHNOLOGIES .....	29

PARENTAL INVOLVEMENT .....	29
PASSWORDS AND PASSWORD SECURITY .....	30
Passwords .....	30
Password Security .....	33
Zombie Accounts .....	34
PERSONAL OR SENSITIVE INFORMATION .....	35
Protecting Personal, Sensitive, Confidential and Classified Information .....	35
Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media .....	35
REMOTE ACCESS .....	36
SAFE USE OF IMAGES .....	37
Taking of Images and Film .....	37
Consent of Adults Who Work at the School .....	37
Publishing Pupil’s Images and Work .....	37
Storage of Images .....	38
Webcams and CCTV .....	38
Video Conferencing .....	39
SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT & REMOVABLE MEDIA .....	37
School ICT Equipment .....	37
Portable & Mobile ICT Equipment .....	37
Mobile Technologies .....	38
Removable Media .....	39
SERVERS .....	40
SMILE AND STAY SAFE POSTER .....	44
SOCIAL MEDIA, INCLUDING FACEBOOK AND TWITTER .....	45
SYSTEMS AND ACCESS .....	47
TELEPHONE SERVICES .....	48
WRITING AND REVIEWING THIS POLICY .....	49
Staff and Pupil Involvement in Policy Creation .....	49
Review Procedure .....	49
CURRENT LEGISLATION .....	50
Acts Relating to Monitoring of Staff eMail .....	46
Other Acts Relating to eSafety .....	46
Acts Relating to the Protection of Personal Data .....	48

## Introduction

ICT in the 21<sup>st</sup> 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, we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

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

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

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

At **Roundwood Park School**, we understand the responsibility to educate our students 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.

Roundwood Park holds personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our 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 Agreements (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

## Monitoring

Authorised IT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any IT authorised staff member will be happy to comply with this request.

IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school's IT facilities; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

IT 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 IT 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 IT equipment may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider.

## Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT 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 students, breaches will be dealt with in accordance with the school's behavioural policy.

---

## Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of Roundwood Park's IT facilities must be immediately reported to the school's relevant responsible person. 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 relevant responsible person. The relevant responsible individuals in the school are as follows: Dean Inns – Network Manager & Tony Smith – Deputy Head/SIRO.

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

## Acceptable Use Agreement: Students – Secondary

### ICT Acceptable Use Policy for Students



- I will only use IT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will respect all the school's computer resources and understand I am liable for the cost of any wilful damage I cause.
- I will not download or install software on school technologies.
- I will only log on to the school network/VLE with my own username and password.
- I will follow all security recommendations as advised by IT Staff and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all IT communications with fellow students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered inappropriate, offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher. I will immediately inform my teacher if I receive any such material from another student.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without permission.

- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.
- I will support the school approach to online safety and not upload or add any images, video, audio or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I will not enter an ICT room without a member of staff present.
- I understand that my area on the network is for storing files related to schoolwork and that this area is subject to checks by IT Support staff.
- I understand that my use of the Internet and other related technologies can be monitored, logged and can be made available to my teachers.
- I understand that these rules are to keep me safe and that if they are not followed, consequences in line with the student code of conduct will be applied and my parent/ carer may be contacted.
- I will not sign up to online services until I am old enough to do so.

### **Bring Your Own Device**

- If I am borrowing devices from the school, I understand that all tablets or laptops remain the property of Roundwood Park School and are on loan to me. I understand that loan devices must be returned on request.
- My own laptop/tablet/smartphone will only be used for learning purposes during school time. Sanctions will apply for inappropriate use of my device during lessons.
- My teacher has full discretion to ask me to put my device away in any lesson or at any time.
- When I bring my own device to school, I am fully responsible for keeping it safe. I will store my device safely when it is not being used (e.g. in my locker).
- I will ensure that my device has a passcode or other locking system to ensure that my personal information remains safe. I will not use another person's device without their permission.

- With my own device, I will only connect to the school WiFi network to use the filtered Internet. I will not enable 3G/4G during school time for my own protection and to protect the privacy of staff and students.
- I will not use any VPN Service or any other software to attempt to bypass the schools filtering and firewall solutions.
- I will not take photographs or videos without the permission of the person concerned. I will not post any images to social media taken during school time without permission. I will delete any image if I am asked to do so by a member of staff.
- While I am allowed to install my own software and media on my own device, I understand that precedence must be given to learning applications.
- My own device must not contain illegal software, must not be 'Jailbroken' and must have regular official updates applied from the manufacturer in order to keep secure.
- If available, I will ensure my device has adequate antivirus and spyware protection and that it is kept up to date to prevent damage to other devices on the school network (e.g. AVG Antivirus).
- Laptops, Tablets and Smartphones may only be used at the discretion of the teacher of the lesson and will be subject to normal school rules unless explicit permission to use them has been granted.
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day.

I understand that my network and Internet access may be taken away if I fail to abide by these rules.

I understand that I am subject to sanctions laid down in the Rewards and Consequences policy and violations of the law may result in police involvement.

Signed (Parent/Carer): .....

Print Name:

.....

Signed (Student): .....

Print Name:

.....

Signed (Deputy Head):



Print Name: Tony Smith

## ICT Acceptable Use Policy for Sixth Formers



### General

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will respect all the school's computer resources and understand I am liable for the cost of any wilful damage I cause.
- I will not download or install software on school technologies.
- I will only log on to the school network/VLE with my own username and password.
- I will follow all security recommendations as advised by IT Staff and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address on the school system.
- I will make sure that all ICT communications with fellow students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered inappropriate, offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher. I will immediately inform my teacher if I receive any such material from another student.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.

- I will support the school approach to online safety and not upload or add any images, video, audio or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that my area on the network is for storing files related to school work and that this area is subject to checks by IT Support staff.
- I understand that my use of the Internet and other related technologies can be monitored, logged and can be made available to my teachers.
- I understand that these rules are to keep me safe and that if they are not followed, consequences in line with the student code of conduct will be applied and my parent/carer may be contacted.
- I will not sign up to online services until I am old enough to do so.

### **Bring Your Own Device**

- If I am borrowing devices from the school, I understand that all tablets or laptops remain the property of Roundwood Park School and are on loan to me. I understand that loan devices must be returned on request.
- My own laptop/tablet/smartphone will only be used for learning purposes during school time. Sanctions will apply for inappropriate use of my device during lessons.
- My teacher has full discretion to ask me to put my device away in any lesson or at any time.
- When I bring my own device to school, I am fully responsible for keeping it safe. I will store my device safely when it is not being used (e.g. in my locker).
- I will ensure that my device has a passcode or other locking system to ensure that my personal information remains safe. I will not use another person's device without their permission.
- With my own device, I will only connect to the school WiFi network to use the filtered Internet. I will not enable 3G/4G during school time for my own protection and to protect the privacy of staff and students.
- I will not use any VPN Service or any other software to attempt to bypass the schools filtering and firewall solutions.

- I will not take photographs or videos without the permission of the person concerned. I will not post any images to social media taken during school time without permission. I will delete any image if I am asked to do so by a member of staff.
- While I am allowed to install my own software and media on my own device, I understand that precedence must be given to learning applications.
- My own device must not contain illegal software, must not be 'Jailbroken' and must have regular official updates applied from the manufacturer in order to keep secure.
- If available, I will ensure my device has adequate antivirus and spyware protection and that it is kept up to date to prevent damage to other devices on the school network (e.g. AVG Antivirus).
- Smartphones may only be used at the discretion of the teacher of the lesson and will be subject to normal school rules unless explicit permission to use them has been granted.
- I will not bring a smart watch to school because I am not permitted to wear one during the school day.

I understand that my network and Internet access may be taken away if I fail to abide by these rules.

I understand that I am subject to sanctions laid down in the Rewards and Consequences policy and violations of the law may result in police involvement.

Signed (Parent/Carer): .....

Print Name:

.....

Signed (Student): .....

Print Name:

.....

Signed (Deputy Head):



Print Name: Tony Smith

# Acceptable Use Agreement: Staff, Governors and Visitors

## ICT Acceptable Use Policy for School Staff, Governors and Visitors

- I confirm that I have read and understood the RPS ICT Policy for Staff and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity, in accordance with the document. In particular:
- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school.
- To protect my own privacy, I will only use a school email address and school telephone numbers (including school mobile phone) as contact details for students and their parents.
- If I use instant messaging, chat rooms, webcams, discussion forums or social media for communicating with students or parents about learning it will only be via the school's VLE or after discussion with senior staff.
- I will reject/refuse invitations or and/or requests from students to partake in discussion forums, instant messaging, webcams and social networking.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school or accessed remotely. Personal data should only be taken off site on removal media as a last resort and should be encrypted if doing so.
- I will not install any hardware or software on the school network without the permission of the IT Support team.
- I will support and promote the school's e-Safety and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will not use my personal mobile phone or other electronic equipment to photograph or video students or staff without permission from the Senior Leadership Team.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will take all necessary steps to ensure that all laptops and memory devices are fully virus protected and that protection is kept up to date.

- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is logged.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset or offend any member of the school community.

I confirm I have read the RPS ICT Policy and the school's Data Protection Policy and will implement the guidelines indicated. In particular:

- Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers must be password protected to meet the school's password policy and will be fully logged off or the screen locked before being left unattended.
- At no time should the school's Management database (SIMS) be left open when I am absent from my workspace, without the screen being locked to prevent a breach of Data Protection laws.
- I understand that I have the same obligation to protect school data when working on a computer outside school and should only access school data by CC4 Anywhere or other authorised methods.
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken I understand that the school may monitor or check my use of IT equipment and electronic communications.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name (print) .....

Date .....

Signed.....

## Staff Professional Responsibilities

The HSCB eSafety subgroup group have produced a clear summary of **professional responsibilities related to the use of IT** which has been endorsed by unions. To download visit <http://www.thegrid.org.uk/eservices/safety/policies.shtml>



### **PROFESSIONAL RESPONSIBILITIES** **When using any form of ICT, including the Internet,** **in school and outside school**



For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.



- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.



- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.



- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.



- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.

- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.

- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.



You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

## 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.
- Never interfere with any anti-virus software installed on school IT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact the IT Helpdesk immediately. The IT Helpdesk will advise you what actions to take and be responsible for advising others that need to know.

## Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Please see Roundwood Park's Data Protection Policy for further information.

---

### 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 concerning 'Safe Handling of Data'
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile IT 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 IT 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 mopers (multi-function print, fax, scan and copiers) are used

---

### Protective Marking

- Appropriate labelling of data should help staff 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

- Roundwood Park uses 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

The trust's Senior Risk Information Officer (SIRO) is Tony Smith (Deputy Head)

The SIRO will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the trust's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

---

## Information Asset Owner (IAO)

The trust has identified Information Asset Owners (IAOs) for the various types of data being held (e.g. student information / staff information / assessment data etc.) These are:

- IT facilities provision and storage – Mr. Dean Inns – Network Manager
- Student information – Mrs. Karin Barton – Students
- Staff information – Mrs. Julie Fox - Personnel
- Assessment data – Mr. Matt Warren – Deputy Head

The identified Information Asset Owners (IAOs) will manage and address risks to the information and will understand:

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

## Disposal of Redundant IT Equipment Policy

- All redundant IT 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 IT 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 IT 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/si2006/uksi_20063289_en.pdf)

[http://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

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

Electricity at Work Regulations 1989

[http://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 a comprehensive inventory of all its IT 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 e.g. 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 IT 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](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](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](http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal)

## E-mail

The use of e-mail within most schools is an essential means of communication for both staff and Students. 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 students need to understand how to style an e-mail in relation to their age and how to behave responsible online.

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

---

### Managing e-mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- 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 students, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- 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 students are advised to cc. the Headteacher, line manager or designated line manager
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value

- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All Students have their own individual school issued accounts which is their responsibility.
- The forwarding of chain emails is not permitted in school. All inappropriate emails should be forwarded to the IT Helpdesk where they will be dealt with accordingly.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.
- Staff must inform (the eSafety co-ordinator or line manager) if they receive an offensive e-mail
- Students are introduced to e-mail as part of the Computing Programme of Study
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

---

## **Sending e-mails**

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

---

## **Receiving e-mails**

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods

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

---

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

- 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:
    - Encrypt and password protect. See <http://www.thegrid.org.uk/info/dataprotection/#securedata>
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt
  - SecureFX should be used for Confidential emails.

## Equal Opportunities

---

### **Students with Additional Needs**

The school endeavours to create a consistent message with parents/carers for all Students and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some students may require additional support or 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 **Tony Smith** 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, Herts for Learning Ltd, 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 students, 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 PSHCE.

---

### 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 students 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 Computing.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Students 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
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an

organisation such as Cybermentors, Childline or CEOP report abuse button

---

### **eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety.
  - New staff receive information on the school's acceptable use policy as part of their induction
  - All staff have been made aware of their 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 eSafety Co-ordinator)
  - All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.
- 

### **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 students at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on

# Incident Reporting, eSafety Incident Log & Infringements

---

## Incident Reporting

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

---

## eSafety Incident Log

The school holds an eSafety Incident Log and all eSafety issues are recorded in this document by the eSafety Co-Ordinator.

---

## Misuse and Infringements

### 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.

### 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 relevant responsible person, and an investigation by the eSafety Co-Ordinator. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- 

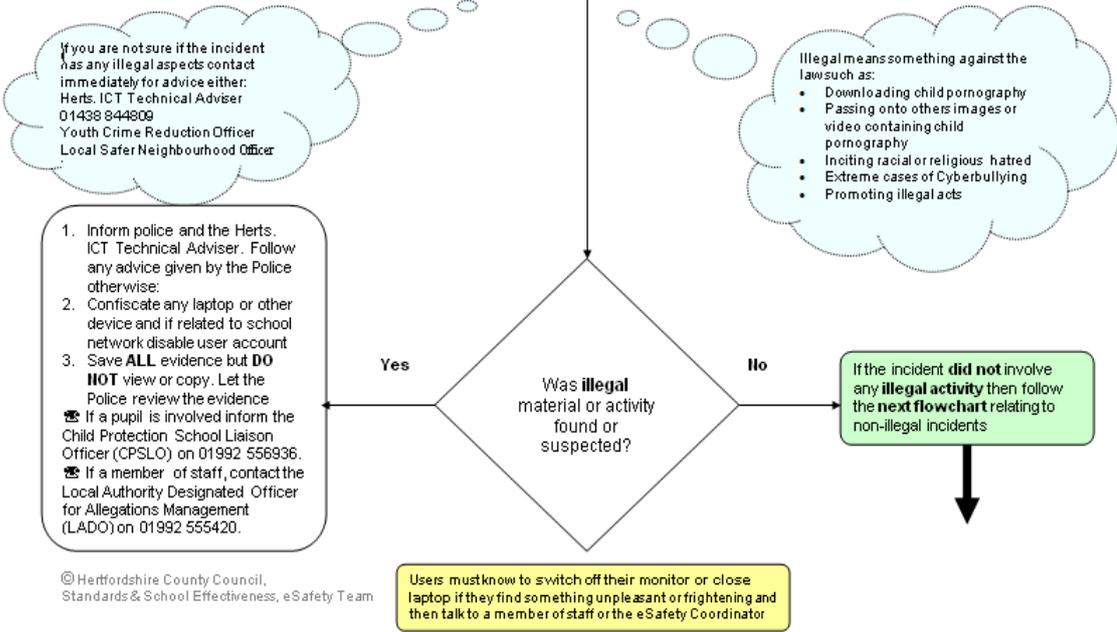
## Flowcharts for Managing an eSafety Incident

These three flowcharts have been developed by the HSCB eSafety subgroup and are designed to help schools successfully manage eSafety incidents

<http://www.thegrid.org.uk/eservices/safety/research/incident.shtml>

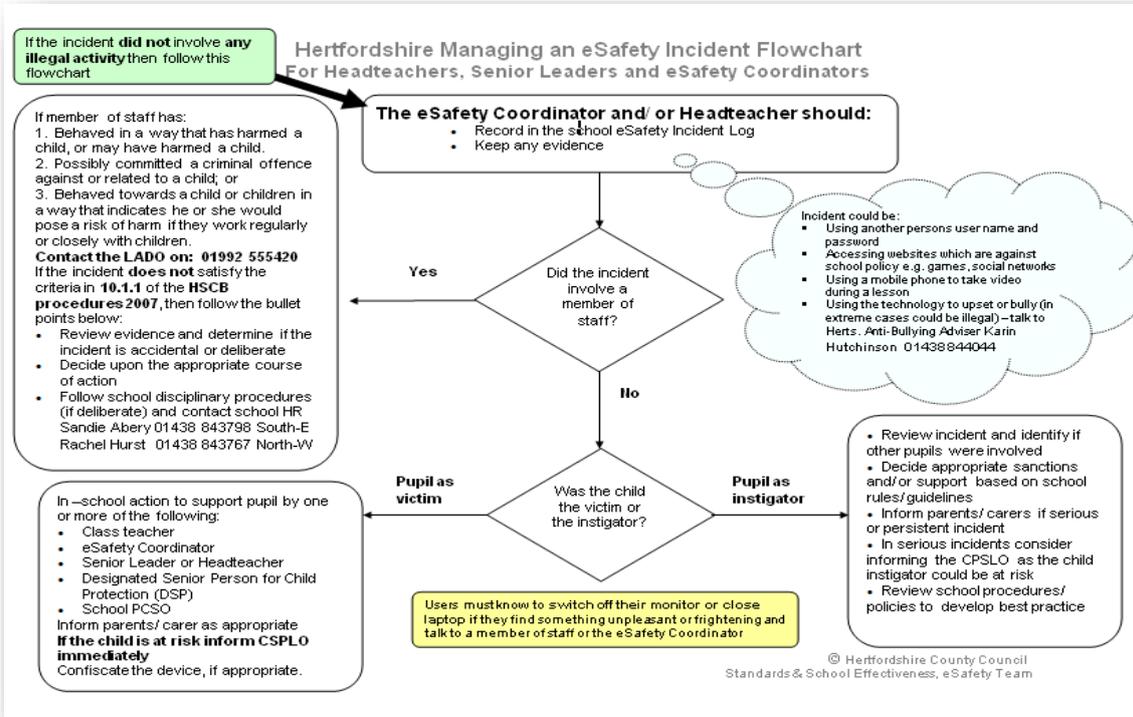
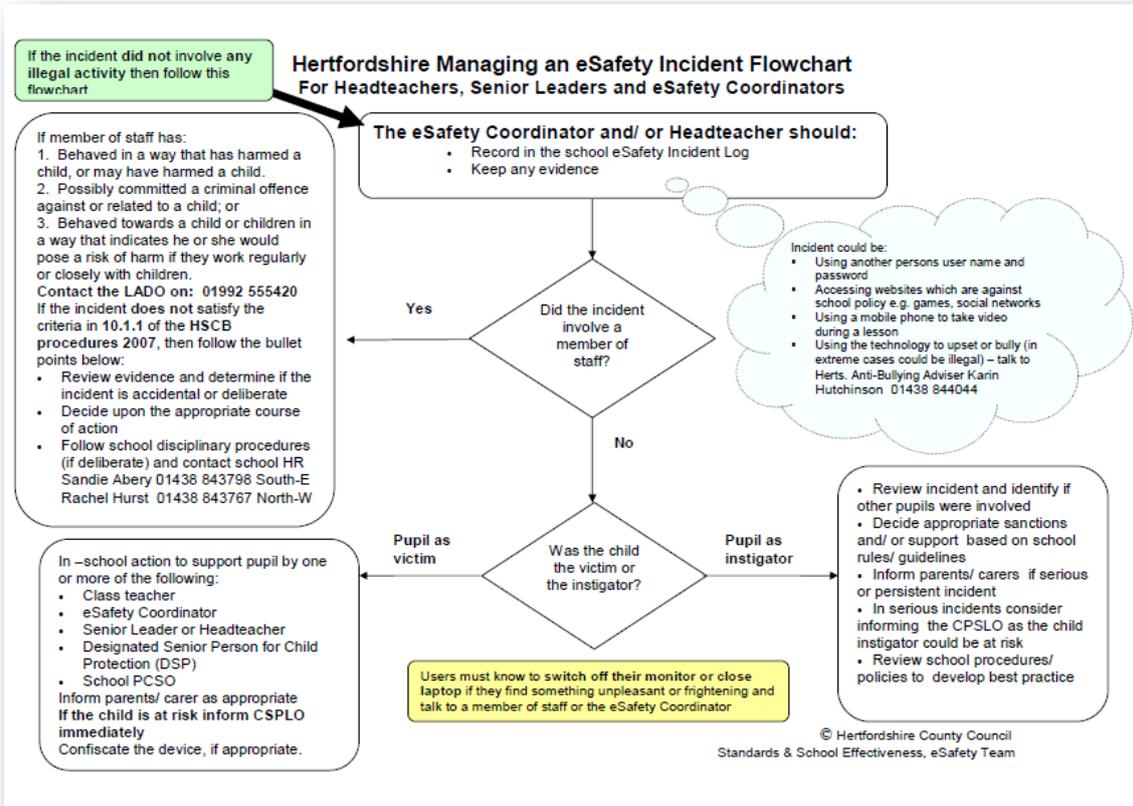
Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident  
For Headteachers, Senior Leaders and eSafety Coordinators

Following an incident the eSafety Coordinator and/or Headteacher will need to decide quickly if the incident involved any illegal activity



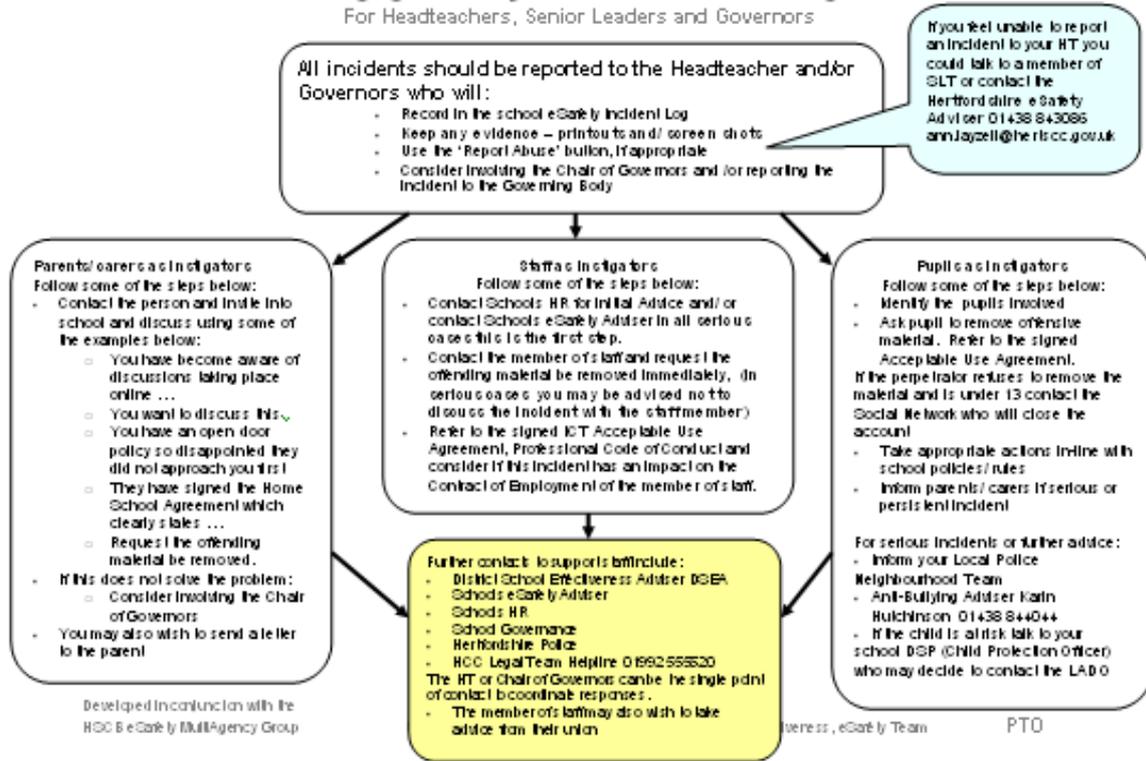
© Hertfordshire County Council, Standards & School Effectiveness, eSafety Team

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



## Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and Governors



## Internet Access

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

---

## Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

---

## Internet Use

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

It is at the Headteacher's discretion as to what internet activities are permissible for staff and students 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 HICS web filtering service.
- Roundwood Park 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 students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students 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
- Students 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 managers to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the **IT Helpdesk** for a safety check first
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from **Network Manager**.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

## Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students 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 and online games websites to students within school
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our students are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Headteacher
- When signing up to online services that require the uploading of what could be deemed as **personal or sensitive data**, schools should check terms and conditions regarding the location of storage. Please see the Safe Harbor Agreement Statement <http://www.thegrid.org.uk/info/dataprotection/#data>  
  
Also: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/>
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored <http://www.coppa.org/comply.htm>

## 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 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 of new technologies, together with the associated risks.

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by *contacting the eSafety Co-Coordinator*.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information evenings
  - Practical training sessions e.g. current eSafety issues
  - Posters
  - School website information
  - Newsletter items
- Parents are asked to sign a Home School Agreement containing the following statements –
- **I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.**
- **I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.**
- **I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat if they are underage (13+ years in most cases).**
- **I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.**

## Passwords and Password Security

---

### Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security

<http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised IT support staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the Network Manager immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and students who have left the school are removed from the system within **24 hours**.

**If you think your password may have been compromised or someone else has become aware of your password report this to your IT 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 students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students 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, VLE and Management Information System (Staff only) log-in username.
- Students are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or VLE, 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 **1 Hour**.
- Due consideration should be given when logging into the virtual learning environment or other online application to the browser/cache options (shared or private computer)
- In our school, all IT password policies are the responsibility of The Network Manager and all staff and students are expected to comply with the policies at all times

---

## **Zombie Accounts**

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorised access (Microsoft® advise every 42 days)

## Personal or Sensitive Information

---

### Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.
- Only download personal data from systems if expressly authorised to do so by your line manager.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling section of the Data Protection policy.

---

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

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

Please refer to the document on the grid for guidance on How to Encrypt Files

- <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

## Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- Remote access should only be via Secure VPN if authorised to do so or CC4Anywhere.

## Safe Use of Images

---

### Taking of Images and Film

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

<http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse>

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher
- Students and staff must have permission from the Headteacher before any image can be uploaded for publication

---

### Consent of Adults Who Work at the School

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

---

### Publishing Pupil's Images and Work

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of Students will not be published. Students' 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 Network Manager has authority to upload to the internet.

---

## Storage of Images

- Images/ films of children are stored on the school's network
- Students 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 students within the confines of the school network or other online school resource

---

## Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are **Dean Inns – Network Manager, Tony Smith – Deputy Headteacher, Myles Hamilton – Lettings Manager, Tim Stanbridge – Premises Manager**
- Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

---

## **Video Conferencing**

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

## School IT Equipment including Portable & Mobile IT Equipment & Removable Media

---

### School IT Equipment

- As a user of the school IT equipment, you are responsible for your activity
- Roundwood Park logs IT equipment issued to staff and records serial numbers as part of the school's inventory.
- Visitors are not allowed to plug their IT hardware into the school network points (unless special provision has been made). They should use the school's wireless facilities wherever possible.
- Ensure that all IT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- Privately owned IT equipment should not be used on a school network without the permission of the Network Manager.
- On termination of employment, resignation or transfer, return all IT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- No personal, sensitive, confidential or classified information is disclosed to any unauthorised person or stored on your Own PC or equipment.
- All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their unit
  - recovering and returning equipment when no longer needed
- All redundant IT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

---

### Portable & Mobile IT Equipment

This section covers such items as laptops, mobile devices and removable data storage

devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile IT 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 IT support team, fully licensed and only carried out by your IT support team.
- In areas where there are likely to be members of the general public, portable or mobile IT 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. Mobile technologies such as Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. 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
- Students are allowed to bring personal mobile phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off.
- This technology may be used 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 iPads 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 or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**' - Page 33

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your IT support team

## Servers

- All Servers are in a locked and secure environment
- Access to the servers is only available to the Network Manager and the IT Support Team.
- All servers are password protected with strong passwords.
- Appropriate security software is installed.
- Backups are encrypted.
- Data is backed up every 2 hours during the school day and at 6 hour intervals outside this time period.

## Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



**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 may 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

## **Social Media, including Facebook and Twitter**

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers.
- The Network Manager is responsible for the RPS postings on these technologies and monitors responses from others.
- Staff are able to setup RPS Twitter in accordance with school guidelines.
- Students are not permitted to access their social media accounts whilst at school
- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law

### **Twitter Guidelines**

Twitter is a 'micro blogging' platform which allows users to post short text messages (up to 280 characters in length). Twitter also allows for the attachment of photos and the embedding of links to other web pages.

### **Departmental Use Guidelines**

- Students and Parents/Carers should be encouraged to follow @RPS[Department]. E.g. RPSICT
- Information regarding special achievements will be published as will other Departmental information such as fixtures and results for the PE Department.
- Changes to the extra-curricular timetable will be published as a matter of urgency.
- Specific students will only be mentioned if they have opted to follow an RPS Departmental Twitter account.
- Mentions of specific students will only be made using their Twitter ID.
- Photographs of students will only be used if permission has been granted by a Parent/Carer and the department account is followed by the student in question and full names will not be mentioned with the photographs.

- Links to interesting articles will be tweeted in order to help develop literacy and enhance learning opportunities.
- A wide range of academic bodies and personalities connected to the academic world will be followed to help widen our students' academic horizons and to promote positive role models.
- Open tweets from followers may be replied to and positive debate encouraged.
- Students and Parents/Carers will not be 'followed' by the ANY Departmental account.
- The Twitter feed will not be used to send 'direct messages'.
- Students will not be allowed to follow staff member's personal accounts.
- Despite encouraging debate - political views, comments and opinions will be avoided.
- School staff will not tweet any Departmental Twitter account from their personal Twitter accounts.
- Due care and consideration must be taken before sending any tweet. Content should only be tweeted if appropriate for a classroom environment.
- In the interests of safeguarding, all accounts will be overseen by the school's Senior Leadership Team.

### **Student/Parent/Carer Use**

Followers of @RPS[*Department*] must read and abide by the terms of this document. Any student that does not comply with the acceptable use policy will be blocked and may be reprimanded in line with the school behaviour policy.

Followers must not abuse this communication facility in any way. This includes sending tweets that may be offensive to others.

Any follower sending inappropriate tweets will be blocked immediately.

Followers must not send 'direct messages' to @RPS[*Department*].

Followers may tweet or reply to @RPS[*Department*] but must understand that a reply may not always be received.

Followers must not apply to follow staff members' private accounts.

All members of the Roundwood Park community are encouraged to follow the school accounts.

Only children over the age of 13 should have access to twitter.

The school expects students to adhere to their parents' wishes regarding their use of twitter.

## Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school IT equipment or your own PC
- Do not allow any unauthorised person to use school IT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school IT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on school systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

## Telephone Services

- You may receive personal telephone calls provided:
  1. They are infrequent, kept as brief as possible and do not cause annoyance to others
  2. They are not for profit or to premium rate services
  3. They conform to this and other relevant HCC and school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times

## Writing and Reviewing this Policy

---

### Staff and Student Involvement in Policy Creation

- Staff, governors and students have been involved in making/reviewing the Policy for ICT Acceptable Use.
- 

### Review Procedure

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

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

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

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

This policy has been read, amended and approved by the staff, head teacher and governors in January 2018.

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

#### ***Sexual Offences Act 2003***

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

*Sexual Crime*” document as part of their child protection packs.

### ***Communications Act 2003 (section 127)***

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

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

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

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

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

### ***Malicious Communications Act 1988 (section 1)***

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

### ***Copyright, Design and Patents Act 1988***

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

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

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

### ***Protection of Children Act 1978 (Section 1)***

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

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

### ***Obscene Publications Act 1959 and 1964***

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

### ***Protection from Harassment Act 1997***

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

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

---

## **Acts Relating to the Protection of Personal Data**

### ***Data Protection Act 1998***

[http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

### ***The Freedom of Information Act 2000***

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

---

## **Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance**

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