E - Safety Policy

Heathcote School and Science College

Approved by:	Governors	**Date:** December 2013	
Last reviewed on:	March 2017		
Next review due by:	March 2020		

Acceptable Use Agreement: Pupils - Secondary

Secondary Pupil Acceptable Use - Agreement / eSafety Rules

1. I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.

2. I will not download or install software on school technologies.

3. I will only log on to the school network/ Learning Platform with my own user name and password.

4. I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.

5. I will only use my school e-mail address.

6. I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.

7. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

8. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

9. 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.

10. Images of pupils 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 the permission of Zoe Cozens

11. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.

12. I will respect the privacy and ownership of others' work on-line at all times.

13. I will never try to bypass any of the security in place; this includes using proxy bypass sites. This security is in place to protect me from illegal sites, and to prevent hacking into other people's accounts.

14. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.

15. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

16. I will never use the internet or other ICT communication to bully or make fun of people. It can have very serious consequences. I will report incidents of cyber-bullying to a responsible adult.
17. I will treat all school equipment with care and respect. I will report any problems to a member of staff.

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Janette Powell School E Safety coordinator.

Please return the bottom section of this form to school for filing.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full via our publications scheme on our website.

...X----------

Pupil and Parent/ carer signature

We have discussed this document and ..... (pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Heathcote School and Science College

Parent/ Carer Signature .....

Pupil Signature .....

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

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

1. I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

2. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

4. I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.

5. I will only use the approved, secure e-mail system(s) for any school business.

6. I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.

7. I will not install any hardware of software without permission of Zaf Rehman

8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

9. Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

10. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

11. I will respect copyright and intellectual property rights.

12. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

13. I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

14. Staff are permitted access their school documents using the secure remote desktop protocol (RDP). Please ensure full compliance with data protection and do not leave your home computer unattended when logged in.

15. It is the duty of staff to support the school's safeguarding policy and report any behaviour (staff or students), which is inappropriate or a cause for concern, to a member of the Leadership Group. This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full via our publications scheme on our website.

User Signature

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

The school

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Computer Viruses

We have relevant protection in place, but due to the nature and emergence of viruses, some can find their way onto our networks. So, if you are using removable devices, always check before you access saved files that no virus is on them. If there is, immediately disconnect and refer the issue to the ICT Technical Support Team. If you become aware of any virus, please communicate this to the ICT Technical Support Team.

1. All files downloaded from the Internet, received via e-mail or on removable media (e.g. USBs, CD) must be checked for any viruses using school provided anti-virus software before using them.

2. Never interfere with any anti-virus software installed on school ICT equipment that you use.

3. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

4. 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.

5. Laptop users shall ensure they update their virus protection at least weekly.

ESafety

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 Janette Powell 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 ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

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

ESafety in the Curriculum

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

1. The school has a framework for teaching internet skills in ICT lessons

2. The school provides opportunities within a range of curriculum areas to teach about eSafety

3. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

4. Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

5. Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities

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

7. Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum eSafety Skills Development for Staff

8. Our staff receive regular information and training on eSafety issues in the form of meetings, briefings, newsletters and website

9. New staff receive information on the school's acceptable use policy as part of their induction

10. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

11. All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

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

2. The eSafety policy will be introduced to the pupils at the start of each school year

3. eSafety posters will be prominently displayed

ESafety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

Heathcote School and Science College
e-Safety Incident Log

Details of ALL e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Misuse and Infringements

Complaints

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

Inappropriate Material

1. 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

2. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

3. Sanctions relating to the misuse or misconduct are detailed in the disciplinary policy

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

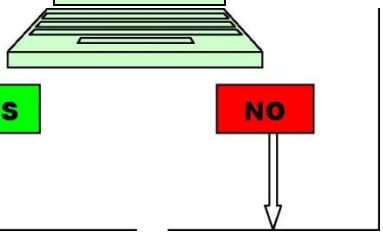
Flow chart to assist SLT and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

^ Still unsure? ^"I

For further advice see a member of SLT/PC Westall who will refer the incident to the appropriate authority

Has illegal activity taken place?



Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to others

Inciting racist or religious hatred
Extreme cases of cyberbullying

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

S Inform PC Katie/Police S Follow the advice given by the Police, or S Confiscate the device and if related to the school network disable user account S Save **ALL** evidence but **DO NOT** view or copy.

Let the Police review the evidence S Refer to Child Protection Officer who will refer to the appropriate authority

Go to next flowchart which outlines the process for non-illegal incidents

Flowchart to assist SLT and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place

The Headteacher/e-Safety Co-ordinator should:

- **Record the incident in the e-safety log**
- **Keep any evidence**

Did the incident involve a member of staff?

YES

If a member of staff has:
Behaved in a way that has, or may have, harmed a child possibly committed a criminal offence
Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children Contact child Protection officer who will refer to the appropriate authority Review evidence and determine whether the incident was accidental or deliberate Decide upon the appropriate course of action Follow school disciplinary procedures

NO

Was the Child the victim or perpetrator?

Pupil as Victim

Pupil as Instigator

Support the pupil by one or more of the following:
Class Teacher e-Safety Co-ordinator Headteacher/Senior Leader Designated Child Protection Officer School Police Officer Inform Parent/carer as appropriate. If the child is at risk contact Child Protection Officer who will refer to the appropriate authority

Incident types could be:
Using another person's user name or password
Accessing websites which are against the schools policy e.g. gaming Using a mobile phone to take video during a lesson
Using technology to upset or bully

Review incident to decide if other pupils were involved
Decide appropriate sanctions
Inform Parent/Carer if serious or persistent incident
If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

Internet Access

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. The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.

All use of the **London Grid for Learning** (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

1. The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

2. Staff will preview any recommended sites before use

3. Personal data sent over the Internet is encrypted

4. Raw image searches are discouraged when working with pupils

5. 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

6. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

7. The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

8. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Internet Use

1. The school's Internet access is designed to enhance and extend education.

2. Internet access is an entitlement for students who show a responsible and mature approach to its use.

3. You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

4. emessages to parents must also be professional and worded appropriately.

5. 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

6. On-line gambling or gaming is not allowed

It is at the Headteachers discretion on what internet activities are permissible for Staff and pupils and how this is disseminated.

Infrastructure

1. Waltham Forest has a monitoring solution via the London Grid for Learning where web-based activity is monitored and recorded

2. School internet access is controlled through the LA's web filtering service.

3. Heathcote School and Science College 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

4. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

5. The school does not allow pupils access to internet logs

6. The school uses management control tools for controlling and monitoring workstations

7. 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

8. 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

9. Sixth form pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the network managers 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 ***(technician/teacher)*** for a safety check first

10. Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from ***(the Headteacher/technician/ICT subject leader)***

11. If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Ict.helpdesk on the internal school system

Managing Other Web 2.0 Technologies

Web 2.0, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

1. At present, the school endeavours to deny access to social networking sites to pupils within school

2. Impero Education Pro e-safety & internet safety software logs and monitor all web activity in real time on all student devices.

3. All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are

4. Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

5. Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

6. Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

7. Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

8. Our pupils are asked to report any incidents of bullying to the school

9. Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

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

1. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

2. 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)

3. Parents/ carers are expected to sign a Home School agreement

4. The school disseminates information to parents relating to eSafety where appropriate in the form of;

   - Website/ Learning Platform postings.
   - Newsletter items

Systems and Access

1. You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

2. Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

3. Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

4. Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

5. 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

6. Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

7. Do not introduce or propagate viruses

8. It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or the Local Authority 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)

9. Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

10. 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

11. It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a 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 of the data.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through ***JLT, staff consultation, governor consultation***

Review Procedure

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

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

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

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

This policy has been read, amended and approved by the staff, head teacher and governors on

Current Legislation

Acts Relating to Monitoring of Staff email *Data*

Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

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

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

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

Other Acts Relating to eSafety *Racial and Religious Hatred Act 2006*

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of

Committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of ***"Children & Families: Safer from Sexual Crime"*** document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 - 3)

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

18. access to computer files or software without permission (for example using another person's password to access files)

19. unauthorised access, as above, in order to commit a further criminal act (such as fraud)

20. impair the operation of a computer or program

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 - 29)

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

offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudophotographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data *Data Protection Act 1998*

http://www.opsi.gov.uk/acts/acts1998/ukpga 19980029 en 1

The Freedom of Information Act 200 http://www.ico.gov.uk/for organisations/freedom of information guide.aspx