

**Stockham Primary School**  
**Acceptable ICT Usage Policy**  
**(September 2016)**

**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, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At Stockham Primary School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

## **Monitoring**

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at anytime without prior notice. If a member of staff is in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the Headteacher.

ICT 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 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 ICT; 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.

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

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

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

## **Incident Reporting**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's ICT Co-ordinator or the Headteacher.

## **Computer Viruses**

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD, memory stick) must be checked for any viruses using school provided antivirus software before using them. School staff must check with the ICT Co-ordinator before using any personal media storage devices.
- Staff must never interfere with any anti-virus software installed on school ICT equipment that they use.
- If anyone suspects that there may be a virus on any school ICT equipment, they should stop using the equipment and contact ICT Co-ordinator/ Technician immediately.
- School staff must not install any software or hardware equipment (including for example memory drives, data storage devices or computer programmes) without the permission of the headteacher.

## **E-mail**

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

## **Managing e-mail**

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- 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.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of a position within school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their 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 pupil e-mail users are expected to adhere to the generally accepted rules particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.
- Staff must inform the Headteacher if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the curriculum.
- However school e-mail accounts are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

### **Sending e-mails**

- Staff and pupils should only use their own school e-mail account so that they can be clearly identified as the originator of a message.
- Senders should keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Senders should 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**

- E-mails should be checked regularly.
- Attachments from an untrusted source should never be opened.
- E-mail systems should not be used to store attachments. Business related work should be detached and saved to the appropriate shared drive/folder

### **Managing the School eSafety Messages**

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

### **Pupils with Additional Needs**

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

### **Incident Reporting**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher.

### **Incident Log**

Some incidents may need to be recorded in other places, for example if they relate to a bullying or racist incident. These must be forwarded to the Headteacher.

## **Misuse and Infringements**

### **Complaints**

Complaints and/ or issues relating to eSafety should be made to the ICT Co-ordinator or Headteacher. All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Co-ordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT 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.
- Users are made aware of sanctions relating to the misuse or misconduct.

### **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.

### **Managing the Internet**

- The school students will only have supervised access to Internet resources through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

### **Internet Use**

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Users must not reveal names of any member of our school community or any other confidential information acquired through the school on any social networking site or blog.
- On-line gambling or gaming is not allowed.

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

## **Infrastructure**

- School internet access is controlled through the Schools Broad Band web filtering service.
- Stockham school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The School does not allow pupils access to internet logs.
- The School uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the ICT Co-ordinator or Headteacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the network 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 teacher for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher or ICT Coordinator.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

## **Use of social media**

Social media, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. Social networking sites, such as Facebook, Twitter, Snapchat and Instagram are well known forms of social media, however this term also applies to other web based services such as blogs, video and audio podcasts, message boards, YouTube and Twitter. It is important to recognise that there are issues regarding the appropriateness of some content and contact with others. To this end, we encourage all members of our school community to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

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

- 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).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web spaces in order to communicate with pupils using the systems approved by the Headteacher.
- In the event that any parent/carer of a child/ren is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.
- In serious cases the local authority will also consider its legal options to deal with any such misuse of social networking and other sites.

### **Staff use of social networking sites**

All school representatives (staff, governors and regular volunteers) have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of the pupils. It is therefore expected that they will adopt high standards of personal conduct, in line with the school's code of conduct for staff and governors. School representatives (including staff, governors and regular volunteers) must always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which may be misinterpreted by others, cause offense to any member of the school community, put at risk child safety or bring the school's reputation into disrepute. This applies to those accessed as part of their professional role as well as outside of school. They must report and record any incident with this potential to the Headteacher.

The following guidance is provided for all school representatives;

- Manage personal information carefully and avoid putting personal information on social networking sites (for example phone numbers, work place, addresses or personal e mail accounts).
- Review carefully any information that is available publicly to ensure that it is accurate and appropriate. For example check any photographs or comments written by others which can be seen by other users.
- Ensure that any security settings are appropriate to prevent pupils or parents accessing personal information.
- School representatives should never 'friend' a pupil, or accept a request to 'friend' a pupil at the school.
- School representatives should avoid being a 'friend' with any parent connected to the school; unless they already have a relationship which is unconnected with their role in the school.
- Confidentiality should be considered at all times and school representatives must ensure that they never place any confidential information on their site

about themselves, their employer, colleagues, pupils, parents or any member of the school community.

- School representatives must never place any comments on line which could be considered derogatory, offensive or that may bring the school's reputation into disrepute.
- School representatives need to ensure that when they are communicating about others, even out of work, that they give due regard to the potential for defamation of character. Making allegations about other employees or members of the school community could result in formal action being taken against them.
- School representatives should not post photographs or video images of school events on line (except on sites approved by the Headteacher such as the school website). School staff should be aware that failure to follow this guidance could result in disciplinary action being taken against them.

### **Parental Involvement**

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

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- Parents/ carers are expected to sign a Home School agreement.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website postings
  - Newsletter items

### **Safe Use of Images**

#### **Taking of Images and Film**

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken

provided they are transferred immediately and solely to the schools network and deleted from the staff device.

## **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 or image 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.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, ie exhibition promoting the school.
- General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

## **Storage of Images**

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

## **Webcams and CCTV**

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs, link schools and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in disciplinary action.

## **School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media**

### **School ICT Equipment**

- Any users of ICT are responsible for any activity undertaken on the school's ICT equipment provided to them.
- The school keeps a log of ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Visitors are not allowed to plug their ICT hardware into the school network points (unless special provision has been made).
- All ICT equipment that should be kept physically secure.
- Staff must 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 all data is saved on a frequent basis to the school's network drive. Staff are responsible for the backup and restoration of any data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines.
- Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment all ICT equipment must be returned to the Headteacher. Staff must also provide details of all your system logons so that they can be disabled.
- It is the responsibility of any member of staff to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorized person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

### **Portable & Mobile ICT Equipment**

- This section covers such items as laptops, tablets and removable data storage devices.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. 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.
- All locally stored data, including diary entries, must be synchronized with the central school network server on a frequent basis.
- Portable and mobile ICT equipment must be made available as necessary for antivirus updates and software installations, patches or upgrades.

- The installation of any applications or software packages must be authorized by the ICT Co-ordinator, fully licensed and only carried out by the school's ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

### **Emerging Technologies**

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

Date agreed by Head Teacher: 7/7/15

Date agreed by Governors: 13/7/15

Date for review: July 2017

## **Current Legislation**

### **Acts Relating to Monitoring of Staff E-mail**

#### **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 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.

For more information [www.teachernet.gov.uk](http://www.teachernet.gov.uk)

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

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

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

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 200**

[http://www.ico.gov.uk/for\\_organisations/freedom\\_of\\_information\\_guide.aspx](http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx)