

Flitwick Lower School eSafety Policy

Contents

Rationale

Roles and Responsibilities

eSafety in the Curriculum

Password Security

Data Security

Managing the Internet safely

Managing other advanced internet technologies

Mobile Technologies

Managing email

Safe Use of Images

Misuse and Infringements

Equal Opportunities

Parental Involvement

Writing and Reviewing this Policy

Appendix 1 Acceptable Use Policy: Staff / Visitors and Governors

Appendix 2 Acceptable Use Policy: Pupils

Appendix 3 BECTA Data Security Do's and Don'ts

Appendix 4 Flowcharts for Managing an eSafety Incident (**To follow**)

Appendix 5 Incident Log

Appendix 6 Internet Online SMART Rules Poster

Appendix 7 Current Legislation

Our e-Safety Policy has been written by the school, building on the Hertfordshire Grid for Learning exemplar policy (with acknowledgement to LGfL, SWGfL and Bristol City Council) and Becta guidance.

Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to 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
- Email 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 Flitwick Lower School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This applies across the school from 4+ to year 4 and is taught and dealt with in an age appropriate manner.

Both this policy and the Acceptable Use Policy (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc). Parents/ carers are asked to read through and sign Acceptable Use Policies with their child on admission to the school. An updated copy of the agreement will be reproduced annually at the start of the Autumn Term and should also be signed on an annual basis.

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

- Information and celebration evenings
- Website postings
- Newsletter items

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 ICT Co-ordinator in our school is also the named eSafety co-ordinator. 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 the LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

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

All users read and sign an Acceptable Use Policy to demonstrate that they have understood the school's e-safety Policy. (Appendix 1 for staff, Appendix 2 for pupils)

Managing the school eSafety messages

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

eSafety skills development for staff

- Staff will receive regular information and training on eSafety issues as new developments occur; All staff will be expected to incorporate eSafety activities and awareness within their curriculum areas.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)

eSafety in the Curriculum

- The school has a framework for teaching internet skills in ICT.
- 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 in an age appropriate manner.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

- Users are provided with an individual network and Learning Platform log-in username. They are expected to use a personal password and to keep it private. 4+ and KS1 pupils use a class log-in and password to access the network.
- Users who believe that their password may have been compromised or someone else has become aware of their password should report this to their teacher (if a pupil), or to the ICT Technician (if a staff member).
- Pupils are not allowed to use the accounts of others, or make any attempt to access on-line materials or files on the school network, of their peers, teachers or others.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed at least once each school term. Individual staff users must also make sure that workstations are not left unattended without being locked.
- Pupils and staff must ensure that they log off the school network at the end of each lesson, or at the end of each day.
- Password should not be saved in the cache when logging on to the learning platform on any computer which is shared.

Data Security

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. Becta defines personal data as “any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, behaviour and assessment records.”

Staff should follow the procedures outlined in Appendix 3 – BECTA Data Security Do’s and Don’ts.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Pupils will have supervised access to Internet resources through the school’s fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator and ICT Technician.
- 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.

Infrastructure

- Flitwick Lower 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.
- School internet access is controlled through the LA’s web filtering service provided by E2BN.
- 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.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator and ICT Technician.
- It is the responsibility of the school, by delegation to the ICT Technician, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines; staff with school laptops will check that updates are being regularly performed.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses carried on such media. It is not the school’s responsibility nor the ICT Technician’s to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to a teacher, or the ICT Technician 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 ICT Technician.
- If there are any issues related to viruses or anti-virus software, the ICT Technician should be informed, preferably by email, or in writing, and no further use of that technology should be made until the issue is resolved.

Managing other Advanced Internet technologies

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

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- 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 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher.

Mobile technologies

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

Personal Mobile devices (including phones)

- The school does not allow pupils to bring in personal mobile phones and devices for their own use during the school day. The school does allow 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.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all permanent staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails 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 email histories can be traced. This 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 email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- If staff are sending emails to parents or pupils, they are advised to cc. the Headteacher, line manager or designated account.
- All pupils have their own individual email accounts allocated on the school learning platform. Only these accounts may be used in school and to send work or file attachments to school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to e mail as a part of their induction in the use of the school's ICT systems in year 3.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. It is therefore not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering any potential harm that might arise.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- 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/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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

Parents/ carers may withdraw permission, in writing, at any time.

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.

The Headteacher must authorise all web site content. This is uploaded by the ICT Technician.

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, laptops) 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/ Learning Platform.

Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes. Pupils will be supervised when using webcams.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an eSafety Incident** should be followed (see appendix 4).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Technician.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Technician, 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 – Appendix 4)

Equal Opportunities

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.

Staff, Governor, Parent and Pupil involvement in policy creation

Review Procedure

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

Staff and Governors have been involved in making / reviewing the eSafety policy through governor and staff meetings; this policy will be reviewed through the same process, 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.

Draft

Appendix 1

Flitwick Lower School

Acceptable Use Policy For Staff / Visitors

The school computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.

Equipment

- Always get permission from the ICT Technician before installing, attempting to install or storing programs of any type on the computers.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Only use school approved and provided mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- Only use the school's digital camera for educational purposes. All photographs should be downloaded onto the school's network, filed by the ICT Technician and only used for internal use. Parental permission must be obtained for external use of photographs. In some circumstances personal digital cameras or mobile phones have been used, ensure all photographs are downloaded onto the school's network as soon as possible and then deleted from your camera or mobile phone.
- During school hours mobile phones must be switched off, or in special circumstances left on silent.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always logoff if you are leaving your computer unattended or have finished using it.
- Students and temporary users will be given a guest logon provided by the ICT Technician.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- The ICT Technician and Headteacher may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' rooms should be avoided.

Learning Platform

- Keep your password to yourself; never use someone else's logon name or password.
- Always logoff if you are leaving your computer unattended or have finished using it.
- You should access the Learning Platform only for school activities.

Email

- Be polite and appreciate that other users might have different views from your own.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

If you suspect or witness a breach of this AUP by another member of staff report it immediately to the ICT Technician, ICT Co-ordinator or Headteacher.

This policy will be reviewed annually.

**Flitwick Lower School
Acceptable Use Policy
For Staff / Visitor**

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____

Signature: _____

Date: _____

Flitwick Lower School Acceptable Use Policy For Governors

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always logoff if you are leaving your computer unattended or have finished using it.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- The ICT Technician and Headteacher may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet via the Learning Platform only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' rooms should be avoided.

Email

- Be polite and appreciate that other users might have different views from your own.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

If you suspect or witness a breach of this AUP by another Learning Platform user report it immediately to the ICT Technician, ICT Co-ordinator or Headteacher.

This policy will be reviewed annually.

Please read this document carefully. If you violate these provisions, access to the Learning Platform will be denied. Additional action may be taken by the school in line with the National Code of Conduct for Governors. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____

Signature: _____

Date: _____

Appendix 2
Flitwick Lower School
Acceptable Use Policy
For Pupils (4+)

The school has computers and Internet access to help us learn.

These rules will keep everyone safe and help us be fair to others.

I will ask a grown up before using the Internet;

I will look after the computer equipment;

I will only use the programs my teacher has told me to;

I have talked about these rules with my teacher and understand what I have to do to use the computers safely.

Pupil Name: _____

Class: _____

Date: _____

Flitwick Lower School Acceptable Use Policy For Pupils (Year 1 and 2)

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

I will ask permission from a member of staff before using the Internet;

I will use only my own login and password.

I will only access my own files;

I will use the computers only for school work;

I will only use programs available to me at school unless I have permission;

I will only use the school's digital camera with permission and under guidance of an adult;

I will only take photographs of people with their permission;

I understand that the school may check my computer files and may monitor the Internet sites I visit.

To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;

I have read and understand the above and agree to use the computer facilities within these guidelines.

Pupil Name: _____

Year: _____ **Class:** _____

Pupil Signature: _____

Date: _____

Flitwick Lower School Acceptable Use Policy For Pupils (Year 3 and 4)

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

I will ask permission from a member of staff before using the Internet;

I will use only my own login and password.

I will only access my own files;

I will use the computers only for school work;

I will only use programs available to me at school unless I have permission;

I will only use the school's digital camera with permission and under guidance of an adult;

I will only take photographs of people with their permission;

I understand that the school may check my computer files and may monitor the Internet sites I visit.

I will only e-mail people I know, or my teacher has approved;

The messages I send will be polite and sensible;

I will only open attachments to emails if they come from someone I know and trust, or my teacher has approved;

I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;

To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;

I have read and understand the Acceptable Use Policy and agree to use the computer facilities within these guidelines.

Pupil Name: _____

Year: _____

Class: _____

Pupil Signature: _____

Date: _____

Appendix 3 BECTA Good practice in information handling: Data security dos and don'ts

We have written this guide for anyone working in a school, college or university who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work. Its aim is to raise your awareness of where potential breaches of security could occur. Following these 'dos and don'ts' will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your organisation may suffer if you lose personal data about individuals.

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

Produced by Becta on behalf of the Department for Children, Schools and Families, these guides have been reviewed and updated with feedback from a number of cross-sector organisations including DCSF, DIUS, JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers.

For further information on these guides, please see <http://www.becta.org.uk/schools/datasecurity> and <http://www.becta.org.uk/feandskills/datasecurity>.

1 Your roles and responsibilities

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

1.1 Important 'dos'

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

1.2 Why protect information?

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

1.3 What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

If you don't already know, find out who is acting as your Information Asset Owner.

1.4 Using protective markings

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed.

Your Information Asset Owner should help you work out how you need to mark the information you view as part of your job. There are different levels of marking depending on how just how sensitive the information is.

1.5 Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

1.6 Working online

1.6.1 Do

- make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT team if you need help.
- only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- make sure that you only install software that your IT team has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your IT team.
- check that your organisation has an acceptable-use policy (AUP)¹ for the internet and ensure that you follow it.

1.7 Email and messaging

1.7.1 Do

- read your organisation's email policy²
- report any spam or phishing³ emails to your IT team that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

1.7.2 Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that your IT team has put in place or recommended
- email sensitive information unless you know it is encrypted⁴. Talk to your IT team for advice.
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails.

¹ See Becta's publication *AUPs in Context: Establishing Safe and Responsible Online Behaviours* [<http://publications.becta.org.uk/display.cfm?resID=39286>].

² See Becta's information on developing e-safety policies [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_pol_03].

³ Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank) [<http://www.google.co.uk/search?q=define%3A+phishing>].

⁴ Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

1.8 Passwords

1.8.1 Do

- follow your organisation's password policy
- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

1.8.2 Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

1.9 Laptops

1.9.1 Do

- shut down your laptop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

1.9.2 Don't

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.

1.10 Sending and sharing

1.10.1 Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them

- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

1.10.2 Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

1.11 Working on-site

1.11.1 Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

1.11.2 Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

1.12 Working off-site

1.12.1 Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

2 Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office [<http://www.ico.gov.uk>].

More detailed guidance for organisations can be found on the Becta website [<http://www.becta.org.uk/plansustainableuccess> and <http://www.becta.org.uk/schools/esafety>].

Test your online safety skills at the Get Safe Online website [<http://www.getsafeonline.org>].

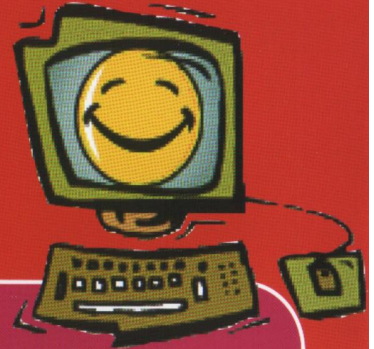
Appendix 5

Flitwick Lower School eSafety Incident Log

Details of ALL eSafety incidents are to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher and any incidents reported to Governors. Any incidents involving cyber bullying should be recorded using the behaviour monitoring system.

Date: Time: When the occurrence took place.	Name of pupil or staff member: Logged by:
Description of the occurrence: (what happened inc. classification of any information compromised)	
Immediate corrective action: (what was done to minimise the impact of the incident)	
Further Action: (tasks to be undertaken to prevent occurrence)	
Advice taken: If yes logged from whom and actions	
Legal implications:	
Closed Date: Date by which the incident was closed by the Head / SIRO	
Signed by all parties involved in incident to clarify actions taken	

internet online smart rules >>>



S **ECRET** *Always keep your name, address, mobile phone number and password private - it's like giving out the keys to your home!*

M **EETING** *Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and with them present.*

A **CCEPTING** *Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.*

R **EMEMBER** *Remember someone online may be lying and not be who they say they are. Stick to the public areas in Chat Rooms and if you feel uncomfortable simply get out of there!*

T **ELL** *Tell your parent or carer if someone or something makes you feel uncomfortable or worried.*

Appendix 7 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.hmsso.gov.uk/acts/acts1998/19980029.htm>

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

<http://www.hmsso.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.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmsso.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

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.