E-Safety Policy

William Fletcher Primary School

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and mobile learning such as touch screen tablets. Computer skills are vital to access life-long learning and employment; ICT is an essential life-skill.

Young people have access to the Internet from many places; home, school, friends' houses, libraries and (for an increasing number of our children) mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not always have these services and has a range of risks associated with its use. School are ideally placed to help young people learn to become "e-safe". This policy is designed to ensure safe Internet use by pupils in school, but also while on-line at home etc.

1. Core Principles of Internet Safety

Internet safety depends on staff, schools, governors, parents and where appropriate, pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones.

There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

2. Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff to enhance the school's management information and business administration systems.

3. How will Internet use enhance learning?

- The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
- Pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
- There is a structured approach to Internet access and Internet searches, with clear progression through the school. This can be seen in the school Computing planning overview.

5. How will filtering be managed?

- The school will work in partnership with parents, Oxfordshire County Council and 123ICT (the school's IT technical support) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the headteacher immediately.
- Website logs will be regularly sampled and monitored.
- The ICT leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

6. How will the risks be assessed?

- In common with other media such as magazines, books and film, some material via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of the Internet content, it is not possible to guarantee that unsuitable material will never appear on the school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher and ICT leader will ensure that the Internet policy is implemented and compliance with the policy monitored.

7. Managing Content

7.1 How will pupils learn to evaluate Internet content?

- School should ensure that the staff and pupils are aware that the use of Internet derived materials should comply with copyright laws.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils to read for information from the web resources.
- Nominated persons (ICT technician) will be responsible for denying additional websites.

- The school web filter will not be removed accept in specific circumstances (eg the viewing of an appropriate video on YouTube).

7.2 How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

8. Communication

8.1 Managing e-mail

- Whole-class or group e-mail addresses only should be used.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must tell their teacher immediately if they receive an offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed notepaper.

8.2 On-line communications and social networking

- Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific lessons learning about the importance of e-safety.
- The use of online chat rooms is not permitted in school, other than as part of an online learning activity (eg project work where children build upon each others knowledge bank through the use of Ipads).

8.3 Mobile technologies

- Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
- Pupil mobile phones are not permitted within the school.

9. Introducing the Policy to Pupils

- Rules for Internet access will be posted in all rooms where computers are used.
- Lessons on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.

10. Parents and E-Safety

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within the school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

11. Consulting with Staff and their inclusion in the E-safety Policy

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School E-Safety Policy and its importance explained.
- The school's consequences for Internet and Mobile phone, tablet misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the "Responsible Internet use" statement before using the Internet resource in school.
- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use will be provided as required.

12. How will complaints be managed?

- Responsibility for managing incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the school's complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- On rare occasions the police may need to be contacted. Early contact could be made to establish the legal position and discuss strategies.

Laptop and Ipad policy for William Fletcher Primary School staff

The laptop / Ipad remains the property of William Fletcher Primary School.

The laptop/ Ipad is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only William Fletcher School Staff should use the laptop/ ipad.

On the teacher leaving the school's employment, the laptop/ Ipad is returned to William Fletcher School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).

When in school and not being used, the laptop/ Ipad must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

If the laptop/ ipad is taken out of school it should not be left in an unattended car. If there is a need to do so it should be locked in the boot.

The laptop/ ipad must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.

Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.

Any software loaded must not affect the integrity of the school network.

If any removable media is used then it must be checked to ensure it is free from any viruses.

It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date.

Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.

Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.

Pupils should not use the staff laptop unsupervised.

If any fault occurs with the laptop / ipad, it should be referred immediately to Stephen Roworth, ICT technician.

When being transported, the carrying case supplied must be used at all times.

The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

Policy for responsible e-mail, network and Internet use for William Fletcher Primary School

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the owner's permission.

- Place inappropriate material onto the Internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregarded my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of William Fletcher Primary School.

2. I will only access the system with my own name and registered password, which I will keep secret.

3. I will inform the ICT School's Technician as soon as possible if I know my password is no longer secret.

4. I will always log off the system when I have finished working. ·

5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.

6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.

7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.

8. I will always adhere to the William Fletcher School Software Compliance Policy.

9. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the ICT technician.

10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.

11. I will report immediately to the headteacher any unpleasant material or messages sent to me.

12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.

13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

14. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.

15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

16. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name.....

Signature: .....

Date: .....

E-Safety Contacts and References

BBC Chat Guide http://www.bbc.co.uk/chatguide/

Becta http://www.becta.org.uk/schools/esafety Childline http://www.childline.org.uk/Child Exploitation & Online Protection Centre http://www.ceop.gov.uk

e-Safety in Schools http://www.kenttrustweb.org.uk?esafety

Grid Club and the Cyber Cafe http://www.gridclub.com

Internet Watch Foundation http://www.iwf.org.uk/

Internet Safety Zone http://www.internetsafetyzone.com/ Kent Primary Advisory e-Safety Pages http://www.kented.org.uk/ngfl/ict/safety.htm

Kidsmart http://www.kidsmart.org.uk/ NCH – The Children's Charity http://www.nch.org.uk/information/index.php?i=209 NSPCC http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm Schools e-Safety Blog http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy http://www.eiskent.co.uk (broadband link) Stop Text Bully www.stoptextbully.com

Think U Know website http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Children's Code of conduct for Internet Use

William Fletcher Primary School

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

Using the Computers:

- I will only access the computer system with the login and password I have been given;
- I will not access other people's files;
- I will not bring in memory sticks or CDs from outside school unless I have my teacher's permission.

Using the Internet:

- I will ask permission from a teacher before using the internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and me;
- I understand that the school may check my computer files and may monitor the internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

Using E-mail:

- I will ask permission from a teacher before sending an e-mail;
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and me;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

Anti-cyber Bullying Policy

William Fletcher Primary School

We aim to ensure that children are safe and feel safe from bullying, harassment and discrimination. Our school is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly.

Cyber-bullying Defined:

Cyber-bullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the Internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Aims of Policy:

- To ensure that pupils, staff and parents understand what cyber- bullying is and how it can be combated.
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying.
- To ensure that reported incidents of cyber bullying are dealt with effectively and quickly.

Understanding Cyber-bullying:

- Cyber-bullying is the use of ICT (usually a mobile phone and or the internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including pupils and school staff.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

Procedures to Prevent Cyber-bullying:

- Staff, pupils, parents and governors to be made aware of issues surrounding cyber-bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff CPD will assist in learning about current technologies.
- Pupils will be involved in developing and communicating this policy.
- Pupils will learn about cyber bullying through PSHE, assemblies, and other curriculum projects.
- Pupils will sign an Acceptable Use of ICT contract.
- Parents will be asked to sign an Acceptable Use of ICT contract and to discuss it's meaning with their children.
- Pupils, parents and staff will be involved in reviewing and revising this policy and school procedure.
- All reports of cyber-bullying will be investigated, recorded, stored in the Headteacher's office and monitored regularly.
- The Local Authority can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents.
- The police will be contacted in cases of actual or suspected illegal

content.

Internet Safety Check

It is good practice to discuss these points with pupils at the start of the school year, the start of a project requiring Internet use, or if revision of acceptable Internet use is necessary.

- Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.
- Only use your own login name and password. Never use another person's details.
- Never give out your address, phone number or arrange to meet someone over the Internet.
- All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message, which could cause upset.
- If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else.
- If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher or to an appropriate member of staff.
- Be aware that the school may check your computer files and monitor the Internet sites you visit.
- Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.
- You and your parents should have signed the school Internet agreement. You will be breaking that agreement if you deliberately break these rules. This could result in you losing your Internet access at school.
- Draw pupil's attention to the poster on the wall in the classroom regarding sensible conduct whilst using the Internet. They can refer to this anytime they need a reminder.

William Fletcher Primary School Guidelines on Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil accidentally finds a website displaying inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting inappropriate materials from the Internet.

Praise the pupil for reporting the incident or explain they should have reported it in line with your school's E-Learning Code of Conduct

-
-
-

Explain to the pupil that, in order to prevent it occurring again, you need to ascertain how the pupil gained access to the inappropriate material

- Ask the pupil to explain what happened

Inform the headteacher and IT Leader so the school Internet filter can be improved accordingly. If appropriate, inform the pupil's parents to explain the preventative action that will taken by the school

The school may produce printed publications and/or a school web site, which may include examples of pupil's work and/or photographs of pupils. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously, which includes the use of images of pupils. Including images of pupils in school publications and on the school website can be highly motivating for the pupils involved, and provides a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents consent to the school publishing their children's work and to the taking and using of photographs and images of their children subject to strict confidentiality of personal information. (This can be changed at any time; just see the Headteacher or ICT Leader).

Digital Video

Digital video is an exciting medium which can motivate and inspire pupils. Research has shown that using digital video in education can help encourage creativity, motivate and enthuse pupils, and improve communication and team-working skills.

At William Fletcher Primary School we intend to use digital video as part of our learning and teaching and for the recording of school productions and events.

We ask that parents consent to their child taking part in the production of digital video, and/or appearing in films.

Whereas the risks of using digital video in education are minimal, schools have a duty of care towards pupils. This means that pupils will remain unidentifiable, reducing the risk of inappropriate contact, if images or examples of their work (including digital video) are used on the school website. All digital video work at William Fletcher Primary School is underpinned by our acceptable use and Internet safety policies.

E-Learning Code of Conduct

Dear Parent/Guardian,

As part of our curriculum we encourage pupils to make use of educational resources available on the Internet. Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials which are inappropriate in school, William Fletcher accesses the Internet by means of Surf Protect, which provides an appropriately filtered service. However, it is not possible to provide a 100% assurance that pupils might not accidentally come across material, which would be inappropriate.

Therefore, in order to allow access to the Internet we would like all pupils to discuss the attached E-Learning Code of Conduct with their parents/guardians and then return the signed form to the school office.

We believe that the educational benefits to pupils from access to the Internet in the form of information resources and opportunities for collaboration far outweigh the potential disadvantages.

During lesson time teachers will guide pupils toward specific materials and educational resources. Where pupils are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in school and use the e-learning resources appropriately.

Yours sincerely

Miss Harvey

ICT Leader