

Box CE VC Primary School

E-Safety and Acceptable use of the Internet Policy

This policy is based on the 'Wiltshire ICT in schools: schools' safety policy 2007 - a template to help schools create their own policy', and the DCFS Cyberbullying - Supporting School Staff, 2009.

This policy should be read in conjunction with other related policies and procedures e.g.

- Child protection policy
- Child protection procedures and record keeping
- Behaviour policy
- Anti-bullying policy
- Esafety policy
- Intimate care and invasive procedures policy
- Disability and equality scheme
- Whistleblowing policy

The internet has become an important aspect of everyday life, to which children need to be able to respond safely and responsibly. At Box Primary School, we believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide. At the same time there are risks that children may gain access to material that is inappropriate. This policy sets out the measures to be taken that minimises these risks.

Our E-safety policy is built on the core principles of the Wiltshire guidance:

Guided educational use

Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will help ensure safe use of the internet.

Risk assessment

As well as the obvious benefits of 21st century technology it also presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to

recognise and avoid these risks - to become 'internet wise'. We in school need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for internet use. Pupils need to know how to cope if they come across inappropriate material.

Pupils may obtain internet access in youth clubs, libraries, and public access points and in homes. Ideally a similar approach to risk assessment and internet safety would be taken in all these locations, although risks do vary with the situation.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit internet access, although it is the appropriateness and consistency of the school's e-safety policy that is of overriding importance.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation., for example children are not allowed to visit online chat rooms at school. Esafety guidelines for pupils, which are agreed by the school council, are prominently displayed in classrooms to help pupils make responsible decisions when using technology.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. *There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.*

Why is the internet important and relevant to our school?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils and staff with quality internet access as part of their learning experience. The school internet access will be designed expressly for educational and professional 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. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised use of the internet

A record will be kept of any pupils who have had their internet access withdrawn temporarily or permanently. Pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.

At Key Stages 1 and 2, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

Internet Filtering

South West Grid for Learning provide a comprehensive filtering system for schools. However if staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet Service Provider (SWGfL) via the Subject Leader or School Leadership Team, using the following contacts:

South West Grid for Learning (SWGfL) Support Team

Telephone: **0870 9081708**

E-mail: **support@swgfl.org.uk**

To notify of an inappropriate website: **abuse@swgfl.org.uk**

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be referred to the Internet Watch.

Assessing Risk

In common with other media such as magazines, books and video, some material available 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 internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire County Council 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 will ensure that the internet policy is implemented and followed with the policy monitored.

Managing Content

Specific lessons will be included within the ICT scheme of work that teaches all pupils how to read for information from web resources. Older pupils should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

The School Website

The point of contact on the website is 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. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Where audio and video are included (e.g. podcasts and video blogging) the nature of the items uploaded will only be included with parental permission.

Electronic Communication

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail and must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone. Sending images without consent or messages that cause distress and harassment to others are considered significant breaches of school conduct.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Online Communication

Students/pupils will be taught about how to keep personal information safe when using online services. Each teacher should make regular and explicit references to e-safety during lessons.

The school will conduct annual pupil surveys about their home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc. The use of online chat is not permitted in school, other than as part of its online learning environment.

Emerging Technologies

As a rule pupils do not need to bring phones to school. If there are extenuating circumstances then the child's teacher will look after the phone for the child,

however as a school we do not accept responsibility if the phone is lost or damaged.

Esafety activities

All Key Stage 2 pupils will use the e-safety activities from the Wiltshire primary schools ICT Scheme of Work and/or the internet Proficiency Scheme, (available from Becta / Grid Club internet Proficiency Scheme) to help teach internet Safety. Every two years the school will have an esafety day which will include an evening session for parents and governors. All parents will receive support information as and when available e.g. Think U Know.

Staff responsibilities

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with a copy of this policy. All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school which is also applicable to the use of a laptop provided by the school, for professional purposes.

Staff should be aware that internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential. Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.

Complaints about e-safety and acceptable use of the internet

Responsibility for handling incidents will be given to the Headteacher, including any complaint about staff misuse. There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies

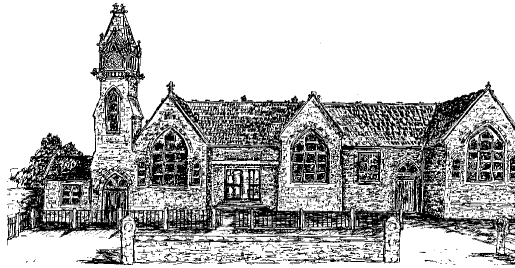
Appendix

1. Responsible Internet Rules
2. Responsible Use Agreement Form for pupils and their parents.
3. Laptop Policy for School Staff

Responsible Internet Use

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

- I will ask permission before using the internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.
- The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.



Box Primary School

Responsible Internet Use

Please complete, sign and return to the school

Name:

Pupil's Agreement

I have read and I understand the school rules for responsible internet Use. I will use the computer system and internet in a responsible way and follow these rules at all times.

Signed:

Date:

Parent's Agreement

I have read and understood the school rules for responsible internet use and I am aware that my child will use the internet during lessons. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.

Signed:

Date:

Please print name:

Box CE VC Primary School Laptop Policy for School Staff

1. The laptop remains the property of Box Primary School.
2. The laptop 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 Box School staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Box 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).
4. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
5. The laptop 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.
6. 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.
7. Any software loaded must not affect the integrity of the school network.
8. If any removable media is used then it must be checked to ensure it is free from any viruses.
9. 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.
10. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. Students must never use the laptop.
13. If any fault occurs with the laptop, it should be referred immediately to the Network Manager.
14. When being transported, the carrying case supplied must be used at all times.
15. 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

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 Box 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 Network Manager/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 Box 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 network manager.
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: