Shoreham Beach Primary School

Computing Acceptable Use Policy

Revised: February 2023

Next revision: February 2025

Networked resources, including Internet access, are available to staff and pupils in the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources.

CONDITIONS OF USE

Personal responsibility
Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of the hardware they are using. Users will accept personal responsibility for reporting misuse of the network to the Head Teacher (in the case of staff) or their class teacher (in the case of pupils).

Acceptable Use
Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines:

TEACHING ABOUT ACCEPTABLE USE OF THE INTERNET

From Year R onwards, the pupils are taught about e-safety using the NSPCC website, and the E-safety tasks built into the Computing schemes of work (NCCE Teach Computing). This includes how they can stay safe when online as well as what is acceptable to write on a computer both in school and at home. Web sites are filtered through two levels of safety (A contracted private company) to try and safeguard children from inappropriate material.

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language- users should remember that they are representatives of the school on a global public system. Illegal activities are strictly forbidden.
3. Do not use any language that could incite hatred against ethnic, religious or other minority groups.
4. Privacy – do not reveal any personal information (eg. Home address, phone number) about yourself or other users. Do not trespass into other users' files or folders.
5. Password- do not reveal your password to anyone. If you think it has been learned by someone else, contact Mike Strugnell.
6. Electronic mail – This is not guaranteed to be private. Messages relating to, or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt others' use.
8. Pupils will not be allowed access to unauthorised chat rooms and should not attempt to access them.
9. Staff and pupils finding unsuitable websites through the school network should report the web address to the Head Teacher or class teacher (in the case of pupils).
10. Take care when using new flash sticks or disks on the network as they may introduce viruses.
11. Do not attempt to visit websites that might be considered inappropriate. (eg. Sites relating to illegal activity. The police or other authorities may be called to investigate such use).
12. Unapproved system utilities and executable files will not be allowed in pupil's work areas or attached to e-mail.
13. Files held on the school's network will be regularly checked by Mike Stugnell.
14. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy ad to ensure that unacceptable use of the internet/intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password where applicable and should not share this information with others. They should log off after their session has finished. Pupils will be encouraged to do the same with increasing accountability for ensuring it is done. User ID and password are taught to pupils at the beginning of Year 1.
- Users finding machines logged on under other users' usernames should logoff the machine whether they intend to use it or not.

- Accessing or creating, transmitting, displaying or publishing any material (eg. Images, sound, data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council has filters in place to block e-mails containing language that is or may be deemed offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law or the Data Protection Act or breaching security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

Users must comply with the acceptable use policy of any other networks that they access.
Users must not download software without approval from the Head Teacher.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform Mike Strugnell or Darren Vallier (HT) immediately if a security problem is identified (or the class teacher in the case of pupils). Do not demonstrate this problem to other users. Users must login with their own user ID and password, where applicable and must not share this information with others. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable IT equipment such as laptops, digital cameras, tablets, microphones, Beebots, etc, are locked away securely in the IT cupboard, or their dedicated secure trolleys, when not in use. Items that need to be left over breaks and lunchtimes should ideally be locked away or at least removed from sight.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs are published. Named images of pupils will only be published with the separate written consent of the parents or carers.

Publishing includes, but is not limited to:
The school website/VLE
The local authority website
Web broadcasting
TV presentations
Newspapers