



City and County of Swansea

A Code of Conduct for Safe use of School ICT Systems



Inset the school badge or logo here	Name of School	
	AUP Version	
	Date of Next Review	

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. These technologies can stimulate discussion, promote creativity and make learning more effective. They also bring opportunities for staff to make learning more engaging and data management more efficient. However, the school is aware that improper use of these systems could expose both the school and the user to potential legal liability. The school will endeavour to ensure that staff and volunteers have good access to ICT to enhance their work and the learning opportunities for pupils in their care. In return the school expects staff and volunteers to agree to be responsible users of ICT.

This Acceptable Use Policy is intended to ensure that:

- staff and volunteers will be responsible users of ICT and stay safe while using the Internet and other communications technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk in their use of ICT in their everyday work.

For my professional and personal safety I understand that:

- the school may monitor my use of the ICT systems, email and other digital communications;
- the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, the Swansea-Edunet Learning Platform) outside the school and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)



Staff Acceptable Use Agreement / Code of Conduct

- I will only use the school's e-mail/Internet/Intranet/Learning Portal and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without the permission of (Name of Network Manager).
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, defamatory or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headteacher.
- I understand that my use of the Internet and other related technologies may be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature **Date**

Full Name

Job title



Passwords

- Always use your own personal passwords to access computer based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Change your password whenever there is any indication of possible system or password compromise.
- Do not record your passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Make sure that logged-on workstations are not left unattended.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, do not disclose your username and password to anyone.
- Select passwords that are not easily guessed e.g. do not use your house or telephone number or choose consecutive or repeated numbers.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with built-in encryption systems.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential or classified data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.



Safe Use of Images

(For advice see the: **Guidance for Schools on Safe Use of Images.**

(<http://www.learn-ict.org.uk/intsafty/index.asp>)

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

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- Ensure that all ICT equipment that you use is kept physically secure.
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

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. Emerging technologies will be examined for educational benefit and the risk assessed before their 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 allows 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.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. 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 images or sound recordings are made on these 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.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any images or sound recordings are made on the devices of any member of the school community.
- 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.

Guidance for staff on the use of Social Networks & Blogs

Social networking sites (e.g. Facebook, MySpace etc.) and blogging sites (e.g. Wordpress, Twitter etc.) are a way of life for many young people and adults. However, adults working with children should review their use of social networks as they take on professional responsibilities. Once published online, information such as photographs and blogs are almost impossible to control. Some adults have been 'caught out' by posting comments or remarks about work or colleagues. It is strongly advised that you make no reference to your school life on these sites or otherwise bring your employer into disrepute.

Acknowledgements

The City and County of Swansea would like to acknowledge the following organisations whose policies and documentation have contributed to the development of this acceptable use policy.

Hertfordshire County Council
The South West Grid for Learning Trust
BECTA

