Acceptable Usage Policy and Staff use of ICT Code of Conduct

Sandra McKenna Head Teacher

December 2022

The Oswaldtwistle School Staff ICT equipment loan Agreement

Use of ICT by school staff

Introduction

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion on educational topics and news.
It also provides and efficient way to access information from the DfES and other government agencies and departments that will help staff to keep abreast of national and local developments.
There are also increasing opportunities for staff to access INSET and Continuing Professional Development activities using the Internet and e-learning resources.
We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Availability
To enable staff to make full use of these important resources, the internet is available to all staff for professional use.
In addition staff must be aware of their own responsibilities when teaching ICT and using it in school.
ICT equipment, which covers the use of digital technologies in school: i.e. email, Internet, intranet and network resources, cameras and camcorders, mobile devices, tablets, usbs, software, equipment including computers and notebooks borrowed from school.

Professional use
Staff model good Internet use where pupils are present, as part of our on-going commitment to encouraging safe and appropriate Internet use by our pupils both in school and at home.
Staff who need support in using the Internet, or who would like INSET in using it more effectively can ask for support from the School Business manager who can arrange training for you.

Personal use
We recognise that staff may occasionally find it useful to use the internet at work for personal purposes, and we understand that encouraging the use of the Internet will help to develop skills and confidence. However, all staff must be aware of the school policy on using Internet facilities for personal use.

OS Making a Difference

The Oswaldtwistle School MAKING A DIFFERENCE
RESPECT • BELIEVE • ACHIEVE • BECOME

Online ordering and shopping

Initiatives such as e-Learning credits and the curriculum online website from the DfES are encouraging schools to use the Internet as an efficient and effective way of ordering resources and materials for teaching and learning. More and more school suppliers now offer discounts for online purchasing of resources, and on-line ordering allows our staff to manage resource purchases more efficiently.

In the light of these developments, our school uses the Internet to order a range of resources and materials. Staff wanting to use this method should first get permission and school guidelines from the head teacher.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool, and we encourage staff to use it where appropriate for communicating with colleagues, organisations, companies and other groups. To facilitate this, staff members will be given a school e-mail address that can be used for professional purposes.

- Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.
- E-mail accounts provided by the school may be occasionally monitored, although personal privacy will be respected.

Online discussion groups, bulletin boards and forum, online chat and messaging (including Twitter, Facebook etc)

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources. Indeed the DfES has held a number of online conferences designed to encourage teaching staff to learn about and use this developing communication technology.

The use of online discussion groups and bulletin boards relating to professional practice and Continuing Professional Development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Portable storage media

Portable media USB memory sticks are a common way of introducing a virus or other undesirable agent into a school computer system.

- Staff will only use external media storage devices supplied by school, or agreed by the ICT coordinator, School Business manager or SLT.

Security and virus protection

The school subscribes to the LEA Antivirus software program, which uses Sophos and Norton Antivirus software. The software is monitored and updated regularly by the school technical support staff. (Bowker IT)

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICTCO/ICT technician.

Staff agreement form

This document covers use of school digital technologies, networks etc both in school and out of school.

Access

- ✓ I will obtain the appropriate log on details and passwords from the ICT Co-ordinator.
- ✓ I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- ✓ If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- ✓ I will not allow unauthorised individuals to access school ICT systems or resources
- ✓ I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- ✓ I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- ✓ I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network
- ✓ I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety coordinator (Data Protection Officer) or member of the SMT. Log with Bowker IT our filtering provider.

Professional Conduct

- ✓ I will not engage in any online activity that may compromise my professional responsibilities
- ✓ I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- ✓ I will never include pupils or former pupils as part of a non-professional social network or group
- ✓ I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities
- ✓ I will not browse, download or send material that could be considered offensive to colleagues
- ✓ I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

OS Making a Difference

The Oswaldtwistle School MAKING A DIFFERENCE

RESPECT • BELIEVE • ACHIEVE • BECOME

Personal Use

- ✓ I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
- ✓ I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- ✓ I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
- ✓ I will not use the school Internet facilities for personal access to public discussion groups or bulletin boards chat rooms or Instant Messaging, for example Facebook, Twitter, Group Chats etc

Email

- ✓ I will only use the approved, secure email system for any school business: (currently: Microsoft office 365)
- ✓ I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

- ✓ I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- ✓ I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- ✓ I will not connect a computer, laptop or other device (including USB flash drive), to the network /Internet that does not have up-to-date anti-virus software.

Teaching and Learning

- ✓ I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
- ✓ I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials
- ✓ I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice
- ✓ I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a classroom with Internet access

Photographs and Video

- ✓ I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- ✓ I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

Data protection/GDPR (General Data Protection Regulation) (May 2018 compliant)

- ✓ I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
- ✓ I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media
- ✓ I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- ✓ I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission
- ✓ I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

- ✓ I will not publish or distribute work that is protected by copyright
- ✓ I will encourage pupils to reference online resources and websites when they use them in a report or Publication

Using New Technology - Hints and Tips for adults working with children and young people

Social Networking hints and tips

Social networking sites are great ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, have a range of privacy settings. These are often setup to 'expose' your details to everyone - anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs, location, etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post potentially embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, Pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Instagram or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.

OS Making a Difference

The Oswaldtwistle School MAKING A DIFFERENCE

RESPECT • BELIEVE • ACHIEVE • BECOME

- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Use location settings wisely. Many social networking and online applications disclose your location. Where this is specifically linked to your identity it will, within a couple of days have disclosed where you live and when you are not at home.
- "I'm attending..." – there are social networking groups to bring together people sharing experiences, such as attending festivals and conferences. Great idea, but don't forget this advertises when you will not be at home.
- Be careful not to leave your Facebook account logged-in in a shared area / household because someone could then leave status messages that may compromise or embarrass you. This is called Frape (Facebook Rape), and can be a form of cyber-bullying.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Think before you post! Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour.
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral rolls and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password(s) – treat them as you would your toothbrush – never share!
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any word found in a dictionary.
- Make sure you have a range of passwords for different circumstances and never use home passwords at work. Make sure you banking password is very 'strong' and never use this for other things!
- Consider using a password safe. You are probably managing a number of passwords and there is Password safe software. It may come with internet security software such as Norton and it comes with browsers such as Chrome.
- Keep all professional work and transactions completely separate from private. Create a web based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.
- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.
- Your school or work laptop (or other equipment) MUST not be used by friends and family.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- Be careful when form filling online…., do you know who the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.
- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.
- Never verify banking details from an email or phone call. Only use the portal and equipment sent directly to you from the Bank / Building Society, or ensure you have validated the information.
- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.
- Popup adverts are often a nuisance. Close them carefully as a 'close' button will often lead you to more advertising as the 'X' might be a graphic.
- If you get an email or advert popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.
- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.
- Use legal sites for downloading music, films etc., such as iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.
- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you

are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.

- Applications like Skype and iPlayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iPlayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible

When you work with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, or interactive whiteboard resource etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home. You are a role model for them so need to model good use of a search engine. Look for opportunities to teach young people how to use search engines effectively.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device.
- You need to be a good role model for copyright. Make sure you use multimedia resources
- Appropriately, don't just 'grab stuff' off the Internet, but, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.
- Think very carefully about sending or posting 'sexy' photos or text to your friends ("sexting") as they can be forwarded with potential very embarrassing outcomes or even cyber-bullying.

Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail. Just delete it!
- Webmail is useful but insecure, and your email address is easily passed on.
- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don't give out your mobile number or home number to students or pupils.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-pass worded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.
- Lock your mobile. Set a pin number or password for your mobile phone. With access to email, social networking and contacts an unlocked mobile phone can put your identity, and others, at risk.

Data Protection Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in

administration and teaching and learning.

We adhere to the LEA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

Staff Laptop / iPad Loans Agreement.

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment or mobile phone must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of **The Oswaldtwistle School** at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage.

They must also agree that, should the equipment be lost or damaged whilst in their personal possession, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement before taking the equipment away from the school premises.

OS Making a Difference

The Oswaldtwistle School MAKING A DIFFERENCE

RESPECT • BELIEVE • ACHIEVE • BECOME