



The Willows School

## Staff AUP

<b>Date Published</b>	<b>September 2023</b>
<b>Version</b>	<b>1</b>
<b>Approved Date</b>	<b>September 2023</b>
<b>Review Cycle</b>	<b>Annual</b>
<b>Review Date</b>	<b>January 2024</b>

An academy within:



“Learning together, to be the best we can be”

## 1. Policy Introduction

This document has been developed to ensure staff within school are aware of their professional responsibilities when using ICT equipment and systems. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage.

## 2. GDPR Updates to Staff AUP

Schools have a duty under the 1998 Data Protection Act to ensure that personal data is stored and accessed securely. Schools also have a need to prepare for the General Data Protection Regulations (GDPR). Personal data includes information in any form (text, images) relating to an identified or identifiable pupil or member of staff. Data protection legislation applies to paper records as well as electronically stored data.

**When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements**

## 3. Staff practices

- 3.1. I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
- 3.2. I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the safeguarding coordinator.
- 3.3. All passwords I create will be in accordance with the school safeguarding Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems and that I will use a unique password for each system.
- 3.4. I will not share my passwords with any colleagues or pupils within school.

- 3.5. I will seek consent from the safeguarding coordinator/ Head teacher/ Senior Information Risk Officer (SIRO) prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- 3.6. I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the safeguarding coordinator/ Head Teacher/ SIRO.
- 3.7. I will take a professional and proactive approach to assessing the effectiveness of filtered internet provision in relation to the educational content that can be viewed by pupils in my care.
- 3.8. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the network manager / safeguarding coordinator/ SIRO (as appropriate)
- 3.9. I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.
- 3.10. I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- 3.11. I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- 3.12. I will secure any equipment taken off site for school trips.
- 3.13. I will only use school-owned or provided portable storage (USB sticks, portable hard drives etc.).
- 3.14. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- 3.15. Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).

- 3.16. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the network manager/ SIRO.
- 3.17. I will return any school-owned ICT equipment or software to the relevant individual within school (network manager) once it is no longer required.
- 3.18. I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- 3.19. I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- 3.20. I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.
- 3.21. Staff should lock computer screens or log-off when away from the computer.

## 4. Social Media

- 4.1. I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- 4.2. I must not use social media tools to communicate with current or former pupils under the age of 18.
- 4.3. I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- 4.4. I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- 4.5. Staff must not access social networking sites for personal use during school working hours.
- 4.6. If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the safeguarding coordinator.

## 5. Managing digital content

- 5.1 I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- 5.2 I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the safeguarding Policy/ Home School Agreement (or any other relevant policy).
- 5.3 Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff. (Safeguarding coordinator or Head Teacher).
- 5.4 When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- 5.5 I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- 5.6 I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.
- 5.7 I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

## 6. Transferring data

- 6.1 Protectively mark documents (electronic or paper) that are sensitive
- 6.2 Do not send sensitive data across unencrypted routes and if no alternative is available, take sensible precautions (e.g. password protect the file and send the password separately) or don't send it.
- 6.3 Never just 'forward' sensitive documents/data out of one email system to another email system without protecting the data. Care should be taken to ensure the email is correctly addressed.

- 6.4 Do not use personal computer systems or personal email addresses; these may not have adequate security protection.
- 6.5 Try to avoid sending anything sensitive by fax (this old technology is still sometimes requested!), be careful to dial correctly and take steps to ensure the intended recipient has received the information as soon as possible after sending the message.

## 7. Learning and Teaching

- 7.1 I will support and promote the school safeguarding policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- 7.2 I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- 7.3 I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

## 8. Email

- 8.1 I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- 8.2 Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- 8.3 I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- 8.4 I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- 8.5 Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the Head teacher, line manager or another suitable member of staff into the email.

- 8.6 I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- 8.7 I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

## 9. Mobile phones and devices

- 9.1 I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- 9.2 Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- 9.3 I will not contact any parents or pupils on my personally-owned device. Unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- 9.4 I will not use any personally-owned mobile device to take images, video or sound recordings.
- 9.5 I will follow the rules about bringing my own personal device into school e.g. smartphone and/or smartwatch.

## 10. Covid 19 related

- 10.1 Staff uploading work for pupils to access in the event of the school /sections of the school going into lock down or a pupil self-isolating for reasons linked to Covid19

## 11. Class Dojo

This part of the policy covers the use of Class Dojo in school and when working from home.

- 11.1 I will only use my school email to set up my Class Dojo account.
- 11.2 I will use a secure password that I will not share with anyone.

- 11.3 I will use my school iPad to communicate with parents initially but make sure that if I have Dojo on my own personal device that it is password protected and can be remotely wiped.
- 11.4 I will follow 'good practice' advice in the creation and use of my password. 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.
- 11.5 I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the school network staff-only drive within school or the school OneDrive.
- 11.6 I will be available to approve and comment on work and reply to messages during our school hours, between 8.00am to 18:00pm, Monday to Friday. This is also at the discretion of each individual.
- 11.7 I will alert the Head of School, Rachael Booth, Designated Safeguarding Lead/ appropriate senior member of staff if I feel an image/video may be a cause for concern.
- 11.8 I will give positive feedback by distributing Dojo points when children complete activities.
- 11.9 I will comment positively and professionally on work that is sent in.
- 11.10 If I receive a message from a parent that is inappropriate, I will alert the Head of School, Rachael Booth.
- 11.11 I will ensure rewards and comments will be distributed fairly.
- 11.12 I will ensure my responses to messages and comments will remain professional and be written in Standard English and be of a professional nature, I will also refrain from using any inappropriate emoji's as part of the messaging element. (Please refer to teachers standards 8.5)
- 11.13 I will ensure that all children in my class have a Dojo account setup and encourage parents to engage in the learning opportunities provided.
- 11.14 I will support my colleagues by contributing to weblinks, videos and images that I will post on my class Dojo story and whole school messages.



## 12. Agreement

I have read and understand all of the above listed points relating to my use of technology within school. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff name

Signed

Date