William Henry Smith School

ICT Acceptable Use Policy

Policy Details

Status:	**In-house**
Frequency of review:	**Annually**
Lead member of staff:	**Caroline Booth**
Last reviewed:	**Autumn term 2019**
Next Review Date:	**Autumn term 2020**
Policy Number:	**WS21**

1.0 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. This document covers Email, Social Media and ICT equipment in general.

The government has placed a statutory duty on schools to help them keep children safe from the risk of radicalisation and extremism. This expectation made clear that every member of staff must be aware of the risks posed by the online activity of extremist groups, and how social media is being used to encourage young people to travel to Syria and Iraq, for example. As a school we undertake regular training and guidance / resources on this area and have a prevent team established. For further information see our Child Protection Policy.

2.0 ICT Equipment and systems

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

- 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.

- 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 eSafeguarding coordinator.

- All passwords I create will be in accordance with the school eSafeguarding 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.

- When using the School wireless system I will adhere to the terms of use I will not share my passwords with any colleagues or pupils within school.

- I will seek consent from the IT Manager prior to the use of any new technologies (hardware, software, cloud-based services) within school.

- 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 IT Manager.

- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.

- 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 IT Manager.

- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with GDPR and any information-handling procedures both on and off site.

- I understand my personal responsibilities in relation to the GDPR and the privacy and disclosure of personal and sensitive confidential information.

- 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.

- I will secure any equipment taken off site for school trips.

- 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.

- 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).

- 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 ICT Manager. Only administrators are able to do this.

- I will return any school-owned ICT equipment or software to the relevant individual within school (ICT Manager) once it is no longer required, or when requested to do so.

- 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 may be reported to the appropriate authorities.

- 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.

- 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.

3.0 Social Media

- I must be mindful that I work in a School environment and others know that and that anything posted can affect the reputation of the school on sites such as Facebook, Twitter and YouTube or any other online publishing websites and that comments made can be interpreted in other ways by others

- I must not use social media tools to communicate with current or former pupils under the age of 18.
I will not use any social media tools to communicate with parents unless approved in writing by the Principal.

- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.

- I must not access social networking sites for personal use during school hours.

- 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 e-safeguarding coordinator or a senior member of staff

- I must make good judgement and consider the reputation of the school in any posts, shares or comments

- What I do during working hours must not be reflected in photographs or posts on my personal social media activities.

- I must not make any derogatory, rude, or threatening/inappropriate comments about the school, or general comments and shares etc. that could bring the school name or values into disrepute or cause upset or offense to others

- I must use social media sites responsibly and ensure that neither my personal reputation or WHSS's is compromised by content, I understand nothing is private on social media

4.0 Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.

- 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 e-safety policy

- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the SLT. Where staff have a part-owned phone they are able to take images but must put them onto the school system ASAP.

- 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.

- 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.

- 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 or internal memory.

- 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.

- I will adhere to the guidelines of Sensitive Information Procedures; using our secure email facility via Office365 to send sensitive information, contracts etc.

- **Monitoring, filtering and flagging of inappropriate and illegal content** – as mentioned further in our e-safety policy to comply with KCSIE and legislations we use Smoothwall web filtering in order to filter this content, furthermore any attempts to access this material by staff or students is flagged up and emailed to IT Support to determine the necessary action (see e-safety flowchart in e-safety policy).

5.0   Learning and teaching

- I will support and promote the school eSafeguarding policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.

- 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.

- I will report any mis-use of equipment or websites immediately to ICT Support.

6.0   Email

- 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.

- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

- 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.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders and likewise not send attachments I am unsure about.

- 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 Principal, line manager or another suitable member of staff into the email.

- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders in order to preserve storage facilities.

- 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.

- Please refer to the WHSS Email guidelines policy for a further breakdown of how to effectively and correctly use the email section.

7.0 Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.   Only staff with permission from the Principal with a phone allowance are exempt.

- 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.

- I will not contact any parents or pupils on my personally-owned device.

- I will not use any personally-owned mobile device to take images, video or sound recordings.

8.0 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. By logging on to the school network for the first time I accept all of the above elements. **Staff are reminded that logging on to the school computer network via wired or wireless means – is your indication that you agree to this policy and any resulting consequences required in terms of breaching them.**

Staff Name	
Signed	
Date	

It is recommended that you read the two documents to familiarise yourself with the functionality and ways of use with regards to our email system and ICT Network.
Both are available from the ICT office and will also be emailed to you.

- New Staff – ICT Induction
- Email – Staff Guidelines
- E-safety Policy
- Sensitive Information Policy
- Any general info