



ACCEPTABLE USE OF IT POLICY



Shirley Infant & Junior Schools

'Every Child, Every Chance, Every Day'

Reviewed By	Russell Hack	Policy Owner	May 2018
Ratified by	Peter Gould	Governor	October 2018
NEXT REVIEW			March 2020

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. People should have an entitlement to safe access at all times.

This Acceptable Use Policy is intended to ensure:

- That people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that everyone has good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users.

Terms of Use

- **Responsibility:** School IT systems must be used in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the IT systems and other users.
- **Monitoring:** The school will monitor use of the systems, devices and digital communications.
- **Vandalism:** Please report any cases of vandalism to the IT support team/School/Trust, and appropriate action will be taken by the school to recover any costs for loss or damage. In case of students vandalising any equipment, parents may potentially be asked to pay for any damaged equipment.
- **Personal Use:** The school systems and devices are primarily intended for educational use and you cannot use them for personal or recreational use unless you have permission.
- **Own Devices:** If allowed to use your own devices in school, you agree to follow the rules set out in this agreement, in the same way as if you were using school equipment.
- **Concerns:** If you have any concerns about the validity of an email (due to the risk of the attachment containing viruses or other harmful programmes), please inform the IT support team immediately.
- **Data Security & Retention:** Data is backed up daily. If you should accidentally delete/lose files in your folder or shared area, please inform the ICT support team immediately so that they can check if it can be recovered.

DOs	DONTs
<ul style="list-style-type: none"> Keep usernames and passwords safe and secure 	<ul style="list-style-type: none"> Do not share it, or use any other person's username and password. Do not write down or store a password where it is possible that someone will steal it.
<ul style="list-style-type: none"> Be aware of "stranger danger", when communicating on-line. 	<ul style="list-style-type: none"> Do not disclose or share personal information about yourself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
<ul style="list-style-type: none"> Report any unpleasant or inappropriate material, messages, or anything that makes you feel uncomfortable when you see it online. 	<ul style="list-style-type: none"> Do not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
<ul style="list-style-type: none"> Respect others' work and property 	<ul style="list-style-type: none"> Do not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
<ul style="list-style-type: none"> Report any damage or faults involving equipment or software, however this may have happened. 	<ul style="list-style-type: none"> Do not take or distribute images of anyone without their permission.
<ul style="list-style-type: none"> Ensure that you use any remote access systems from safe locations where you cannot compromise any sensitive information that you may need to access 	<ul style="list-style-type: none"> Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
<ul style="list-style-type: none"> Ensure that unattended workstations are logged off or locked to ensure children/adults cannot access sensitive data or the internet without supervision (closing laptop lids is sufficient for class computers). 	<ul style="list-style-type: none"> Do not use any programmes or software that might bypass the filtering/security systems in place to prevent access to inappropriate content.
<ul style="list-style-type: none"> Staff to notify of change in circumstances e.g. address/bank details annually 	<ul style="list-style-type: none"> Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email.
<ul style="list-style-type: none"> Use secure systems for file transfers and/or sharing. Where possible keep all files stored on the school network and provide the location to the person so they can access it from there, rather than emailing the document. 	<ul style="list-style-type: none"> Do not send emails with personal details that could identify a data subject
<ul style="list-style-type: none"> Take responsibility for their own use of new technologies, making sure they use technology safely, responsibly and legally. 	<ul style="list-style-type: none"> Do not forward emails to home computers or personal email addresses
<ul style="list-style-type: none"> Be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies. (See our e-Safety Policy and the pupil's e-safety rules.) 	<ul style="list-style-type: none"> Do not leave documents in vehicles
	<ul style="list-style-type: none"> When using social media, do not share information that can identify a data subject without permission

School Specific Systems

Internet

- Staff must ensure that pupils are supervised at all times when using the internet.
- All internet activity should be appropriate to staff's professional activity or the students' education.

- Staff may use the internet facilities for non-business research or browsing outside of the school day (08:30-15:30) so long as said use does not interfere with those working and complies with the Acceptable Use Policy.
- Copyright, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, terrorist, discriminatory, criminal skills related, illegal drugs related or offensive material.
- Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The internet must not be used to engage in any activity for personal gain.
- To ensure compliance with the Acceptable Use Policy for web browsing and email the school reserves the right to monitor and record user activity.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviour of others. As soon as possible, concerns must be shared with the Head of School to investigate.

Social Networks, Chat Rooms, Instant and Text Messaging

- Staff must ensure pupils are taught safe and responsible behaviours whenever using ICT, by supporting and promoting the school's e-Safety policy.
- Staff must ensure that pupils are only given access to secure, age-appropriate chat rooms and social networks, which are approved within an educational context and moderated by a teacher, or approved adult.
- No online activity or applications accessed by users at any time may be used to bring the school, its members, or their own professional role into disrepute. Please also see the Social Networking Policy.

Email

You will be provided with an email address by the School, and the expectation is that you will use this facility for legitimate educational and research activity. You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place.

Remember when sending an email to:

- Be polite - never send or encourage others to send abusive messages.
- Use appropriate language - remember that you are a representative of the School on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
- Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
- Consider the file size of an attachment, files exceeding 1MByte in size are generally considered to be excessively large and you should consider using other methods to transfer such files.
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the School network

Remote Access

The school offers remote access to staff members, and appropriate use of this technology is important.

The remote access system will enable users to access their documents and some school programs from anywhere they have internet access. Users are expected to use the remote systems in a safe and secure manner ensuring all data is kept secure and on the school storage systems for backup and compliance. School data must not be stored on any system other than issued equipment.

All issued laptops will be encrypted and the IT support team will be able to track the device when it is off the school premises.

Any breach or misuse of this technology will lead to disciplinary procedures.

School Website

- Only the designated staff members within the school may upload material to the school website and all material for the website must be monitored and approved by the persons responsible. The user name and password must not be given to any other members of staff or pupils.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes, i.e. school website, will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photographs alongside full names, addresses, telephone numbers or email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website.

Printers and Consumables

A printer security and accounting system is in operation across the school. Staff are provided with a code/badge that they must keep private and use it to release the print jobs. You must use the printers sparingly and for school purposes only. If you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the school.

Staff must not allow students to use their badges/codes to access the printers.

Data

- Users must ensure that personal data (such as the data held on SIMS and the EYFSP) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations.

Usage of school systems is subject to agreement to abide by this policy and any breach of the conditions will be dealt with in line with the school disciplinary procedure:

- A warning
- A removal of access to services and/or devices i.e. internet, email, school computers and mobile devices
- Consequences such as an official warning added to personnel file

In more serious cases or persistent breaches of this policy:

- Report to the school Governors
- Report to appropriate external agencies like the Police, CEOP or Trade Union
- Disciplinary action for staff

This policy should be read in conjunction with the Hamwic Data Protection Policy, Privacy Notice & the E-Safety Policy which can be accessed on the Policies folder.