


Shirley Warren Primary and Nursery School	Effective Date:	May 2023
Policy and Procedure Statement		
<b><u>Acceptable Use of ICT</u></b> <b><u>Policy</u></b>	Revision Date:	May 2024
	Page	1 of 10
	Approval by the FGB	16/25/23
	Signed	
Head Teacher	Mrs Zoe Newton	
Business Manager	Claire Hughes	

To make sure that we protect and educate pupils and staff in their use of technology, you must comply with this policy and the guidelines in it.

The policy includes requirements for all users in connection with:

- online safety
- social networking
- data protection
- confidentiality

Following this policy is a condition of employment in the school and breaches of it may lead to disciplinary action. It is also a condition of being a volunteer in this school and breaches of it may lead to a volunteer being asked to leave.

## General ICT Use

### Personal Use of Equipment

You should not use any school provided ICT equipment for social networking purposes.

In addition, **you should not** make use of school owned equipment for activities which:

- take place at the expense of contractual hours
- relate to a personal business interest
- otherwise contravene anything in this policy

The school will monitor the use of school owned ICT equipment. If you use school owned computer equipment for any of the aforementioned activities, you will have the equipment withdrawn and may face disciplinary action.

If you use school owned ICT equipment away from the school site, you must make sure that no unauthorised or inappropriate use is made of that equipment. You are personally responsible if someone else uses such equipment.

### **Use of personal equipment**

Staff should not have phones on them during work hours around the school unless with specific permission from the Headteacher. Staff may use their phones within the staff room. All Nursery staff phones are securely locked away during contact sessions.

**You should not** use personal equipment (phones, tablets etc) to take photos of children for school purposes or personal use.

All personal equipment, capable of taking photos or videos (i.e. mobile phones), must be kept securely out of the classroom.

### **Installation of Software**

You do not have the access rights to install software on school owned ICT equipment and you should not attempt to circumvent this restriction. Only authorised software which the school is licensed to use is installed on school owned ICT equipment.

In addition, you should be aware that installing software licensed to the school on computers not owned by the school is a breach of copyright and is illegal.

### **Internet Access away from the school**

You can connect school owned ICT equipment to home networks (either wired or wireless) so that you can access the internet; this should be done using either an Ethernet cable from a router or a wifi connection.

You must make sure that your home wifi connection has appropriate security encryption (at least WPA2). If you have to enter a password to access your home wifi, then it's likely this system is already in place.

### **Acceptable Behaviour when Accessing the Internet**

**You must not** do any of the following when accessing the internet on school owned equipment:

- Create, use, transmit or encourage material which:
  - is illegal, obscene, libelous or otherwise defamatory
  - is offensive, threatening or annoying

- o infringes another person's copyright
  - o transmits unsolicited commercial or advertising material
- Obtain unauthorized access to the school's, the City Council's or another organisation's ICT facilities
- Violate other people's privacy.
- Use facilities which do not serve the school's business functions, such as social networking or live chat, message boards, playing games.
- Engage in illegal activities including breaching the Data Protection, Computer Misuse, Obscene Publications Act and Design Copyright and Patents Acts.
- Download copyrighted or confidential information.
- Wilfully disrupt other users' work in any way, including by viruses or data corruption.
- Express personal views which could be misinterpreted as those of the school or the City Council
- Commit the school or City Council to purchasing or acquiring goods or services without proper authorisation.
- Mention work on social media in either a positive or negative context - even after leaving/termination of contract.

**You have a duty to whistleblow any suspected misuse**, whether accidental or deliberate, by reporting it to the Headteacher or the Chair of Governors. Where necessary, the school or City Council will advise on the correct course of action and may further investigate sites, possibly involving the police and disciplinary action.

### **Offensive and Inappropriate Material**

The use of school owned equipment to access, store, copy or distribute items which are inappropriate, offensive, libelous (or in some other way illegal) or may jeopardise security in any way is prohibited. You should be aware that to do so could constitute a prosecutable offence under UK law as well as leading to disciplinary procedures.

### **Removable Media**

The use of removable media, including memory sticks (also known as USB keys), CDs and DVDs to name but a few, carry inherent risks.

- You must only use a memory stick that has been supplied by Shirley Warren Primary & Nursery School for work related purposes.
- You can store non-confidential data on the memory stick for transfer to another desktop or laptop. Please see below for the types of information that you are not allowed to store on the memory stick.
- If the information that you need to store could damage the Council in any way if it fell into the wrong hands, you should secure it. This is to prevent the data

from being accessed by unauthorised personnel should you be unfortunate enough to lose the stick or it is stolen from you. If you are not sure about the nature of the data that you wish to store on your memory stick, please ask for advice from your manager.

- When you connect your memory stick to your SCC desktop, you must virus check any files that are stored on it.
- Take great care to ensure that the memory stick remains safe at all times.

#### **You must not:**

- Store personal, sensitive personal, commercially confidential, or other sensitive or high risk information on your memory stick, including data that may be considered to be confidential under the Freedom Of Information Act, even if it has been secured.
- Use your own personal memory stick or any other removable media device (eg: an iPod) to store any category of school data, non-confidential or otherwise.
- Copy any software that is covered by a license agreement onto any memory stick.
- Upload any unauthorised software onto the school network from a memory stick.
- Upload any virus or malware (malicious software) onto the school network from a memory stick.
- Copy any data onto a memory stick that you have not been authorised to use.

You have a duty to whistleblow any suspected misuse, whether accidental or deliberate, by reporting it to the Headteacher or the Chair of Governors. Where necessary, the school or City Council will advise on the correct course of action and may further investigate sites, possibly involving the police and disciplinary action.

## **Social Networking**

(This section of the policy is based on the Southampton City Council Model Policy) This section sets out the school's recommendations and requirements for the use of social networking media by its employees. In doing so, the school seeks to achieve an appropriate balance in the use of social networks by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to. Whilst the school does not discourage staff from using such sites in their personal time, it does expect certain standards of conduct to be observed in order to protect the school and its reputation, and also to protect staff from the dangers of inappropriate use.

**Accessing social networking sites in working time and/or from school owned ICT equipment is strictly forbidden, whether the equipment is used at home or at school.**

- This means that, for example, you must not access any social networking sites on your work laptop, even when using it at home.
- It also means that you must not access any social networking sites during your working hours, even on equipment that you own, such as your own mobile phone.

As using the school owned equipment and/or network to access such sites is prohibited, these requirements **also apply** to the use of social networking applications by **school staff** in their **own personal time, using their own ICT equipment via the school's internet connection.**

### **Definitions**

The term *employee* or *staff* covers all employees/staff of the school, including casual staff and agency employees. Where individuals from partner organisations are involved in acting on behalf of the school, they will also be expected to comply with this Policy.

Social networking applications include, but are not limited to:

- Social Networking (e.g. Facebook, Instagram, Snapchat)
- Media sharing services (eg. YouTube)
- Micro-blogging applications (e.g. Twitter)
- Online discussion forums and opinion sites (e.g. Mumsnet)
- Blogs
- Messaging - WhatsApp, Facebook Messenger

### **Exceptions**

Social sites which **can** be used in school time and using school owned equipment, **specifically for producing content for the school, and using a school issued user ID and password**, are as follows:

- **Blogger** - we use Blogger to produce the Shirley Warren blog. This may be used with your Shirley Warren ID and password only.
- **Team drive on Google** - we use Team drive on Google to store photos for the blog. This may be used with your Shirley Warren ID and password only.
- **YouTube** - we use YouTube to upload school video and share it on our website or blog. All videos are unlisted and may only be accessed when embedded on a school page. This must be without adverts or suggested videos. Used with your Shirley Warren ID and password only.

## Friends/Befriending

- The school **prohibits staff** from accepting invitations to “friend” **current or past pupils, or pupils’ family members/friends.**
- **You must not initiate friendships with current or past pupils, or pupils’ family members/friends, under any circumstances.**
- If you maintain social network friendships with colleagues, **you must** follow the rules on **Content of Interactions** below.

## Content of interactions

- You **must not** make any reference (whether positive or negative) on social networking sites to the school, your work, the school’s employees, pupils, and their families- this includes naming your place of work on social networking sites.
- You **must not** post information on a social networking site which is confidential to the school, its employees, its pupils or their families.
- You **must not** post entries onto social networking sites which are illegal, derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the school into disrepute.
- You **must not** use the School logo on your own personal social networking accounts, and should not post any photographic images that include pupils.
- When posting any information onto a social networking site, you are recommended to consider whether any entry you make puts your effectiveness to perform your normal duties at risk.
- If you feel aggrieved about some aspect of your work or employment, there are appropriate informal and formal avenues, internally within the school, which allow you to raise and progress such matters. You **must not** raise such matters on social networks. You should discuss any concerns with the Headteacher in the first instance. Guidance is also available from HR/Payroll and trade unions.
- If you become aware of any posting on a social network which breaches these guidelines, either because you see it publicly available, or because you are “friends” with a colleague who has posted it, **you have a duty to whistleblow** to either the Headteacher or the Chair of Governors.
- If you become aware that any pupil has made inappropriate/insulting/threatening comments about pupils, families or staff or made derogatory comments about the school, **you have a duty to whistleblow** to either the Headteacher or the Chair of Governors.

## Security

- **You must** check your security profiles and privacy settings on any social networks that you use. If you are not clear about how to restrict access to your content, you should regard all content as **publicly available** and act accordingly.

- When using social networking sites, you are recommended to only post content that you would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible. You should consider not only how content could reflect on yourself, but also on your professionalism and the reputation of the school as your employer.
- Even with privacy settings in place it is still possible that your personal details may be accessed more broadly than you assume.
- Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

## Data Protection and Confidentiality

The school recognises that staff, governors, parents and pupils have a right to have information about them kept up-to-date and confidential. The section makes sure that we comply with our registration with the [Information Commissioner](#).

### Discussing Pupils, Families, Governors and Staff

- Discussions among staff, governors or volunteers about others should be purposeful and professional - this will avoid discussions which could be classed as malicious or gossip.
- **You must never** discuss pupils or staff in the hearing of anyone who does not have the right to receive such information.
- If discussing a pupil in emails, only use initials with a brief comment.
- **Staff and governors must use** school email address for school related purposes. It is **not** acceptable for any staff or governors to use personal email accounts to discuss any school matters.
- **You must only share** confidential information with people who have a right to receive it.
- If you become aware that confidential information is being shared openly or incorrectly, **you have a duty to whistleblow** to either the Headteacher or the Chair of Governors.

### Recorded Information

- Recorded information of a confidential nature concerning staff, governors, volunteers, pupils or families is kept in locked cabinets or on an encrypted system such as CPOMs or school's encrypted drives.
- **You must not** leave information unsecured or lying around.
- Confidential information on computer systems is controlled by usernames and passwords.

- **You must lock** computer screens when leaving them unattended.
- **You have a duty** to make sure changes to your own personal information are passed to the Admin Manager.

### **Safeguarding Information**

- **You must** refer to the school's Safeguarding policy and your own Safeguarding Training in connection with this section of the policy.
- **You have a duty** to report Safeguarding concerns.
- At Shirley Warren, we use CPOMS and body maps for recording safeguarding concerns.
- The **DSL's must** make sure the information received is dated and clearly documents concerns regarding the risk identified.
- Safeguarding information is kept on encrypted software within CPOMS. Confidential files predating CPOMS are kept in a locked cabinet.
- Safeguarding information must only be stored on CPOM systems .

### **Transfer of Information**

Confidential information about staff, governors, volunteers, families or pupils will be transferred to people outside the school under the circumstances listed below:

- When disclosure is required by a warrant or a court order.
- When the Headteacher or DSL considers that a non- disclosure would pose a serious risk to the welfare of a child, employee, governor or volunteer. No data protection law prevents this.
- When an employee, governor or pupil leaves or moves to a new school or employer.
- When transferring information you must take care to make sure that it is accurate.
- When transferring information to outside agencies, you must check the credentials of those who will receive the information. If there is any doubt, you must not transfer any information to them.
- Where confidential information is transferred by post, it should be clearly addressed to the person who has the right to receive it and mark it Confidential. You should consider using a tracked service, such as recorded or guaranteed delivery. All procedure within SCC Guidance and Retention of Child Protection Records and Welfare Records must be followed



- You should only transfer information electronically by AnyComms ([www.securesouthampton.co.uk](http://www.securesouthampton.co.uk)). The Headteacher, Admin Manager and Inclusion Manager have access to this system.
- You must not include personally identifiable information in emails, or in attachments to emails.
- Where the information is transferred by phone, you should take a person's number, verify it, and call them back.
- Admin staff must send common transfer forms (CTF) for pupil data will be transferred electronically using the DfE secure website.
- When information is picked up in person, eg. when a cohort of children transfer to secondary school, you must only release it to an authorised person and obtain a signature.

### **Retention of Records**

Records of pupils must be kept whilst the child attends the school. After this time, any relevant records must be transferred to the pupil's future school. Any confidential information that is not relevant and therefore not transferred must be disposed of confidentially.

Records of employees and governors must be kept whilst a person is employed at the school. After this time, any relevant information must be passed to the employee's new employer. Any confidential information that is not relevant and therefore not transferred must be archived, if required, or disposed of confidentially.

### **Internal Information**

The content of staff meetings, internal communications and staff notice boards is classed as confidential information and must be treated as such according to this policy.

## **Responsibility and Accountability**

### **Headteachers/Managers**

- **must make sure** that all existing and new staff are familiar with this policy and its relationship to the school's standards, policies and guidance on the use of ICT.
- **must provide** opportunities to discuss appropriate social networking use by staff on a regular basis, and make sure that any queries raised are resolved swiftly.
- **must make sure** that any concerns raised in connection with this policy are investigated promptly and appropriately, in accordance with the School's Disciplinary Procedure and Code of Conduct and Disciplinary Rules.

### Employees and Volunteers:

- **must make sure** that they are familiar with the contents of this policy and its relationship to the school's standards, policies and guidance on the use of ICT.
- **must raise** any queries or areas of concern they have relating to the use of social networking sites and interpretation of this policy
- **must comply** with this policy

### HR/Payroll:

- Will advise and support headteachers and line managers on the application of this policy.

### Governors:

- Will review this policy and its application every two years
- Must make sure that their own conduct is in line with that expected of staff, as outlined in this policy.

### Policy Breaches:

If you are found to be in breach of this policy, you may be subject to disciplinary action, in accordance with the School's Disciplinary Policy and Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal.

Where you work in roles that are governed by professional bodies/professional codes of conduct, the professional rules relating to social networking applied to them may be more stringent than those within this Policy. You are advised to consult such advice (eg. from your own union).

**I have read and understood the ICT Use Policy**

Signed \_\_\_\_\_ (member of staff)

Print Name \_\_\_\_\_

**Please sign one copy and return to the office. Keep the other copy.**