



# Information Communication Technology

## ACCEPTABLE USE POLICY

| Versio<br>n | Date       | Amended<br>by   | Comments                                                                                                                                                                                                      | Approved | Review<br>Date |
|-------------|------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------|
| V2.0        | Sept<br>23 | J.<br>McLellan  | Inclusion of need for staff to report data breaches and to send messages to parents/carers via the Portal.<br>Filtering section changed to include collaboration with The Technology Team rather than the LA. |          | Sept 24        |
| V3.0        | Sept<br>24 | Megan<br>Davies | Reviewed legislation<br>Adapted lay out<br>Updated to meet monitoring and filtering.<br>Change co head to head                                                                                                |          | Sept 25        |

## **SOUTHROP C OF E PRIMARY SCHOOL**

### **Information Technology ACCEPTABLE USE POLICY SEPTEMBER 2024**

#### **Contents:**

Statement of intent  
Legal framework  
Roles and responsibilities  
Definitions  
Unacceptable use  
Staff  
Pupils  
Parents  
Data security  
Internet access  
Monitoring and review  
Appendix 1: Facebook Guidelines for staff

#### **1. Statement of intent**

Southrop C of E Primary School recognises that ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors, who have access to and users of the school's ICT systems, both in and out of our setting.

Breaches of this policy may be dealt with under our Code of Conduct Policy

This document complies with the requirements set out in the UK GDPR and Data Protection Act 2018

#### **2. Legal Framework**

This policy has due regard to legislation including, but not limited to, the following:

- Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- DfE (2023) 'Data protection in schools'
- DfE (2018) 'Data protection: a toolkit for schools'
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- (DfE) Searching, screening and confiscation: advice for schools
- (DfE) Keeping Children Safe in Education 2024

This policy will be implemented in accordance with the following school policies and procedures:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Data Protection Policy
- Freedom of Information Policy
- Cyber-security Policy
- Online Safety Policy
- Staff Discipline Policy
- Code of Conduct Policy

### **3. Roles and responsibilities**

The governing board has overall responsibility for:

- Monitoring the implementation of this policy and all relevant procedures across the school.
- Arranging training for all relevant staff that is appropriate to their role.
- Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to, ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Having regard to 'Keeping children safe in education' when making arrangements to safeguard and promote the welfare of children.

The Head Teacher will hold the overall responsibility for this policy and for ensuring it is implemented correctly.

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of current school e-safety policy and practises.
- They have read and understood the appropriate ICT agreements
- They report any suspected misuse or problem to the Head teacher.

- Digital communications with students are only on a professional level and carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities

## 4. Definitions

**"ICT facilities"**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

**"Users"**: anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

**"Personal use"**: any use or activity not directly related to the users' employment, study or purpose.

**"Authorised personnel"**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

**"Materials"**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

## 5. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head Teacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

### **Responding to incidents of misuse**

It is hoped that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, through deliberate misuse. Depending on the misuse the Headteacher will inform the relevant authorities immediately of any concerns of infringements.

## **6. Staff**

### **Access to school ICT facilities and materials**

The school's technology manager, The Tech Team, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Headteacher.

### **Use of phones and email**

#### **Staff E-mails**

The school provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided. Where possible staff members should use the portal system to contact parents. Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender

should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Head teacher immediately and follow our data breach procedure.

### **Use of Mobile Phones**

Staff must keep their mobile phones away during school hours, either in their bags or in the staff room. If Staff are awaiting a call that is an emergency they must inform the Headteacher.

Personal phones must not be used for school matters, unless special permission has been given by the Headteacher – this might be granted on school trips. Staff must keep a record of the numbers they call, who they spoke to, the purpose and the duration of the call.

### **Use of Smart Watches- Children**

Children are not allowed Smart Watches as these can be used in the same way as mobile phones. If a child does have a smart watch they will be asked to give it in to the office where it will be securely locked away until the end of the day when it can be collected. The same applies to a child if they need a mobile phone in school for the journey home. The school does not take any responsibility for these items during the day

### **Use of Smart Watches – Staff**

Staff must ensure that if they are wearing a smart watch that all notifications are turned off. If a member of staff or child requires a smart watch for medical purposes then this will be discussed with the Headteacher and built into the individual's medical plan.

### **Personal use**

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Head teacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during school hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5).

Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

### **Personal social media accounts**

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

### **Remote access**

We allow staff to access the school's ICT facilities and materials remotely through Uniquity and The Portal. Staff using ICT remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Head teacher may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

### **School social media accounts**

The school has official Facebook accounts managed by the Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account. The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

### **Monitoring of school network and use of ICT facilities**

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

## **7. Pupils**

### **Access to ICT facilities**

Pupils will access to a range of IT equipment in school; ipads and laptops.

Children are responsible for ensuring that:

- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They will be expected to know and understand the school policies and also know and understand the policy of taking/use of images and on cyberbullying.
- They should understand the importance of adopting good e-safety practice when using digital technologies out of school.

### **Search and deletion**

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching.

### **Unacceptable use of ICT and the internet outside of school**

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

## **8. Parents**

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and devices in an appropriate way. The school will therefore take every opportunity to help parents understand how to support their children through communications and the website.

### **Access to ICT facilities and materials**

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Head Teacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

### **Communicating with or about the school online**

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels. We ask parents to sign the agreement on the portal.

## **9. Data security**

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

### **Passwords**

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

### **Software updates, firewalls, and anti-virus software**

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

### **Data protection**

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

### **Access to facilities and materials**

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices. Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

### **Encryption**

The school ensures that its devices and systems have an appropriate level of encryption. School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

## **10. Internet access**

The school wireless internet connection is secured.

### **Visitors**

Visitors to the school will not be permitted to use the school's wi-fi unless specific authorisation is granted by the Headteacher. The Headteacher will only grant authorisation if visitors need to access the school's wi-fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

## **11. Monitoring and review**

This policy will be reviewed every three years by the Headteacher. The next scheduled review date for this policy is September 27. Any changes made to this policy will be communicated to all members of staff and the governing board.



## **Appendix 1**

### **Facebook Guidelines for staff**

#### **DO NOT ACCEPT FRIEND REQUEST FROM PUPILS ON SOCIAL MEDIA**

#### **10 Rules for school staff on Facebook**

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

#### **Check your privacy settings**

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.

Don't forget to check your old posts and photos – go to [bit.ly/2MdQXMN](https://bit.ly/2MdQXMN) to find out how to limit the visibility of previous posts.

The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster.

Google your name to see what information about you is visible to the public.

Prevent search engines from indexing your profile so that people can't search for you by name – go to [bit.ly/2zMdVht](https://bit.ly/2zMdVht) to find out how to do this.

Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

## **What do to if...**

### **A pupil adds you on social media**

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.

Notify the senior leadership team or the Headteacher about what's happening

### **A parent adds you on social media**

It is at your discretion whether to respond. It is recommended that you don't accept friend requests from parents. When deciding bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

### **You're being harassed on social media, or somebody is spreading something offensive about you.**

**Do not** retaliate or respond in any way. Save evidence of any abuse by taking screenshots and recording the time and date it occurred. Report the material to Facebook or the relevant social network and ask them to remove it. If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you your Head teacher should consider contacting the police.