



# ICT and internet acceptable use policy

**Approved by:** Governing Body

**Last reviewed on:** Summer Term 2023

**Next review due by:** Summer Term 2025

# Contents

1. Introduction and aims .....	2
2. Relevant legislation and guidance .....	2
3. Definitions .....	3
4. Unacceptable use .....	3
5. Staff (including governors, volunteers, and contractors) .....	4
6. Pupils .....	6
7. Parents .....	7
8. Data security .....	7
9. Internet access .....	8
10. Monitoring and review .....	9
11. Related policies .....	9
Appendix 1: Facebook cheat sheet for staff .....	10

---

## 1. Introduction and aims

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.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct/etc.

## 2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- › [Data Protection Act 2018](#)
- › [The General Data Protection Regulation](#)
- › [Computer Misuse Act 1990](#)
- › [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](#)
- › [Keeping Children Safe in Education 2018](#)
- › [Searching, screening and confiscation: advice for schools](#)

### 3. Definitions

- › **ICT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, internet, 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 or study
- › **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

### 4. 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 (see section 4.2 below).

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 any device which is approved must have up to date anti-virus software installed and any personal data stored must be encrypted
- › Setting up or installing 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.

#### **4.1 Exceptions from unacceptable use**

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the head teacher's discretion.

The Head teacher's approval must be given in writing in advance after consultation with ICT support.

#### **4.2 Sanctions**

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour/discipline/staff discipline/staff code of conduct/etc.

## **5. Staff (including governors, volunteers, and contractors)**

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

The school's ICT manager & SBM manage 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 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 ICT manager or SBM.

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

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. Or via the School's communications system (currently Schoolcomms/parentpay)

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/or password protected 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 School Business Manager immediately and follow our data breach procedure.

Staff are reminded that they are representing the school and communications must reflect this

## 5.2 Personal use

Staff are permitted to occasionally use school internet or device for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The ICT Manager/SBM or Headteacher 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 working 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). Nor must they store work related information or data on personal devices.

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 (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

### 5.2.1 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).

## 5.3 Remote access

The school may allow you to take home a laptop or device which has been allocated to you for working at home.

***No item may be borrowed or taken away from school without first asking for permission and signing a loan agreement. Please see School Business Manager who maintains the school's asset register.***

Staff accessing the school's ICT facilities and materials 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 ICT manager/SBM or 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.

Please see Data Protection Policies on school website or ask if you are unsure.

## 5.4 School social media accounts

The school has an official Facebook/Twitter page, managed by ICT Manager. 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.

## 5.5 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

## 6. Pupils

### 6.1 Access to ICT facilities

- › Computers and equipment are available to pupils only under the supervision of staff.
- › Pupils must abide by the ICT responsible use guidance.

### 6.2 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 or break the school's rules.

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

The school will sanction pupils, in line with the behaviour/discipline 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

## 7. Parents

### 7.1 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.

### 7.2 Communicating with or about the school online

We believe it is important for pupils to 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 expect that pupils and parents will;

Be respectful towards members of staff, and the school, at all times be respectful of other parents/carers and children.

Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

## 8. 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.

### 8.1 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.

Passwords should be changed on a regular basis or when compromised.

## **8.2 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.

## **8.3 Data protection**

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

Please refer to Data Protection and associated policies available to view on School Website.

## **8.4 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.

These access rights are managed by ICT Manager and School Business Manager.

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 ICT Manager/ School Business Manager 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.***

## **8.5 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 head teacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

## **9. Internet access**

The school wireless internet connection is secured.

- Filtering is used to prevent access to inappropriate sites
- The password is protected and should not be disclosed to pupils or unauthorised persons

The school is aware that filters are not always fool-proof and if you do accidentally access, then this should be reported immediately to ICT Manager/School Business Manager or Head teacher.

### **9.1 Parents and visitors**

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the head teacher.

The head teacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)



- › 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)

***Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.***

## **10. Monitoring and review**

The Head teacher and ICT Manager/School Business Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

## **11. Related policies/codes**

This policy should be read alongside the school's policies on:

- Online safety

  - Safeguarding and child protection

  - Behaviour

  - HR / Staff policies re discipline/conduct

  - Data protection

- Professional codes of Conduct

## Appendix 1: Facebook cheat sheet for staff

### Don't accept friend requests from pupils on social media

#### 10 rules for school staff on Facebook

1. Consider modifying your display name – use your first and middle name, or 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 Head teacher about what's happening

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

- › It is at your discretion whether to respond. 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 or a senior leader should consider contacting the police