



# The Oak Partnership

## ICT Acceptable Use Policy

We are committed to safeguarding ensuring the health, safety and well-being of all pupils in accordance with safeguarding procedures and guidance for staff outlined in the schools' Health and Safety, Child Protection, Security and Safeguarding policies.

# ICT Acceptable Use Policy

## Document Information

	Information
Document author:	COO
Review date:	17 December 2025
Approved by:	Board of Directors
Adopted by:	Board of Directors
Publication date:	September 2019
Next Review date:	December 2026
Review schedule:	Annual
Distribution:	Trust Intranet and all staff
Document status:	Version 3.0

## Version Control

Version	Issue Date	Amended by	Comments
1.0	2019	N/A	Original
2.0	December 2024	COO	Large scale updates to reflect technology developments and news risks.
3.0	December 2025	COO	Expectation for annual sign off added. Clarity around data breaches added. More detail about ICT monitoring systems added.

## Contents

Scope of Agreement.....	3
Definitions.....	3
General Responsibilities.....	3
TOP staff personal phones / devices .....	3
TOP work phones / devices .....	4
Volunteers, visitors and contractors' (and anyone else otherwise engaged by the school) phones / devices .....	4
TOP email accounts .....	4
Email monitoring.....	5
Third party access to email .....	5
Retention and deletion of email accounts .....	5
Technical Infrastructure .....	6
Passwords .....	6
Filtering .....	6
Online professional and personal safety .....	6
Cyberbullying.....	7
System and Data Security:.....	7
Training.....	7
Reporting Incidents.....	8

### Scope of Agreement

This Acceptable User Policy (AUP) applies to all staff, volunteers, local school committee members, directors and visitors who have access to the TOP's ICT systems and to work related use of ICT systems outside of their main place of work. The Trust reserves the right to use reasonable professional judgement to determine whether any act or behaviour not in this policy is considered unacceptable use of the Trust's ICT facilities and therefore fall within the scope of this policy.

### Definitions

**ICT systems:** 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 that may become available in the future which is provided as part of the Trust's ICT service

**Devices:** iPad / tablet / laptop / mobile phone / all devices with imaging and sharing capabilities / USB devices.

**Staff:** A term which in this policy includes employees and all volunteers including all layers of governance.

### General Responsibilities

Staff, volunteers and visitors who have access to and are users of TOP's ICT systems are expected to:

- Use TOP's ICT systems in a responsible way.
- Report any illegal, inappropriate or harmful material, data breaches, suspected misuse or concerns about the use of ICT to a senior leader or Trust COO or Data Protection Lead
- Model the safe use of ICT
- Refrain from publishing any information that: may be offensive to colleagues, may breach the integrity of the ethos of TOP or may bring the trust into disrepute (this includes personal sites)
- Protect own professional identity online by ensuring security settings for social networking sites are enabled fully.
- Ensure acceptable use of social media.
- Respect copyright.

### TOP staff personal phones / devices

- Staff are not permitted to use personal phones / devices while pupils are present.
- Staff personal phones / devices should be locked or stored away in school during pupil contact time.
- Staff use of personal phones / devices is restricted to non-contact time, and to areas of the school where pupils are not present.
- Personal phones / devices should not be used to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.

## *ICT Acceptable Use Policy*

- In the event of a personal mobile needing to be used for work related activity such as two-factor authentication, this should be done with transparency with the device being securely stored after use.
- If access to a personal phone / device is required in the classroom for medical purposes, this will be with the full knowledge and agreement of the senior leadership team and will remain away from pupil access. The phone / device will never be accessed when pupils are present except in circumstances of medical emergency. Personal phone / devices could be subject to monitoring and review by the senior leadership team.

### **TOP work phones / devices**

- Some members of staff are provided with a phone or device by TOP for work purposes 'a work phone / device'.
- Only authorised staff are permitted to use work phones/devices, and unsupervised access to those devices must not be provided to anyone without Trust authorisation.
- Work device functions must only be used for work purposes; this includes making/receiving calls; sending/receiving emails; two-factor authentication; app use; internet use; camera use or any other communication.
- Staff must ensure that all use, communication and conduct linked to a work phone / device is transparent, appropriate and professional, and adheres to the TOP staff code of conduct and trust policies.

### **Volunteers, visitors and contractors' (and anyone else otherwise engaged by the school) phones / devices**

- All persons visiting an Oak Partnership school must comply with the school's procedures of being a phone free zone unless there is a legitimate business reason for not doing so. Examples of legitimate business reasons are, but not limited to: building condition photography, to provide a quotation for works, two-factor authentication, logging work undertaken on site.
- The person visiting must seek approval from a senior leader if they have a legitimate business reason to carry a phone/device on the school site.
- Where permission is granted for a phone/device to be carried on the school site, either
  - The person visiting will need to be escorted by a member of staff for the duration of the visit.
  - Or, where the person visiting cannot be escorted or it is not practicable, they will be required to:
    - share their device camera roll prior to leaving site on request

### **TOP email accounts**

Office 365 email services are provided to Oak Partnership employees/volunteers to support the organisation's primary purposes of education and its associated business functions.

- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

## *ICT Acceptable Use Policy*

- 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 that contains the personal information of another person, they must inform a senior leader immediately and follow our data breach procedure by informing our Data Protection Lead (Barney Rycroft) as soon as the breach is discovered.

### **Email monitoring**

- TOP reserves the right to access employee email accounts, records and content of emails sent and received by employees where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of the organisation's rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate.
- Email accounts may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights. The Data Protection Lead should be informed and give permission for an employee's mailbox to be accessed.

### **Third party access to email**

- Where an employee/volunteer is absent from work for an unexpected or prolonged period, TOP reserves the right to grant access to their email account for business continuity purposes.
- Access will normally be granted to the employee/volunteer's line manager.
- As soon as it is practicable and appropriate, the user of the email account will be notified.
- Where access is granted to an employee/volunteer's email account under these circumstances, it will be made clear that emails marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

### **Retention and deletion of email accounts**

- When an employee or volunteer leaves TOP, their email account and network access will be disabled from the date of their last working day.

## *ICT Acceptable Use Policy*

- Where there is an identified business need, TOP reserves the right to grant access to an employee/volunteer's email account and files for a period of time after the leaving date. Access will normally be granted to the employee/volunteer's line manager.
- Employees/volunteers are encouraged to delete any personal emails, such as payslips, pensions correspondence, from the email account before their leaving date and to notify the pension provider of an alternative email address.
- The email account will be fully deleted once the retention period has passed as defined in TOP's email retention schedule.

### **Technical Infrastructure**

Staff, volunteers and visitors who have access to and are users of TOP's ICT systems should not try to by-pass any of the technical security measures that have been put in place by the Trust. These measures include:

- the proxy or firewall settings of the Trust network (unless permission has been granted)
- not having the rights to install software on a computer (unless permission has been granted)
- not using removable media (unless permission has been granted)

### **Passwords**

Staff, volunteers and visitors who have access to and are users of the TOP's ICT systems should ensure that:

- Username and passwords are not shared with anyone else and are protected from unauthorised disclosure.
- Passwords are stored securely.
- The same password must not be used across different accounts or applications.
- Default passwords must be changed.

### **Filtering and Monitoring**

The use of TOP's ICT, digital technology and communication systems will be monitored. This monitoring is sometimes device specific and will involve capturing data (e.g. key strokes and screen shots) and sending real-time alerts to school leaders. Staff, volunteers and visitors who have access to and are users of TOP's ICT systems should ensure that:

- They do not try to by-pass the filtering and monitoring system used by the Trust (unless permission has been granted)
- If special access is granted to sites that are normally filtered, the computer / device should not be left unsupervised.
- Any filtering issues should be reported immediately.

### **Online professional and personal safety**

Staff, volunteers and visitors who have access to and are users of TOP's ICT systems are expected:

- To report all online safety incidents to the relevant senior leader.
- To be professional in all communications and actions at all times when using TOP's ICT systems. Communications should not use aggressive or inappropriate language.
- To not engage in any on-line activity that may compromise professional responsibilities.
- To only use chat and social networking sites in work in accordance with the Trust's policies.

## *ICT Acceptable Use Policy*

- To only communicate with pupils, parents/carers, and colleagues using official trust/school systems. All communication should be professional in tone and manner.
- To be aware of the risk of using personal email addresses, mobile phones and social networking sites for such communications.
- To not input sensitive or personal or sensitive data into AI tools.
- To not use online gambling, inappropriate advertising, phishing and/or financial scams

### **Cyberbullying**

- TOP has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- Any incidents of bullying should be reported in accordance with Trust procedures.

### **System and Data Security:**

Staff, volunteers and visitors who have access to and are users of TOP's ICT systems are expected:

- To not access, copy, remove or otherwise alter any other user's files, without their express permission.
- To only use apps/ software that store learner information once authority from a senior leader has been given – to ensure the right data protection impact assessment has occurred.
- To not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted. Any concerns about the validity of an email should be reported immediately due to the risk of the link or attachment containing viruses or other harmful programmes.
- To not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. To not try to use any programmes or software that might allow a user to bypass the filtering / security systems in place to prevent access to such materials.
- To not disable or cause any deliberate damage to Trust equipment, or the equipment belonging to others.
- To ensure personal devices are protected by up to date anti-virus software and are free from viruses when using them in work or when visiting another TOP site.
- To only transport, hold, disclose or share personal data in accordance with the TOP Data Protection Policy (or other relevant policy).
- To keep all staff, pupil, parent/carer data and other sensitive data private and confidential, except when it is deemed necessary or required by law or by Trust policy to disclose such information to an appropriate authority.

### **Training**

Staff, volunteers and visitors who have access to and are users of TOP's ICT systems are expected to:

- Participate in cyber security training on an annual basis.
- Participate in any other training where there is an identified knowledge or skills gap.
- Sign off reading and understanding this policy on an annual basis.

### **Reporting Incidents**

- Any illegal, inappropriate or harmful material, data breaches, security incidents, suspected misuse or concerns about the use of ICT should be reported immediately to a senior leader or the trust COO.
- Any incidents should be recorded in accordance with TOP procedures.
- In some cases, the Police may need to be informed.
- Any suspicious emails that could represent a cyber-threat should be reported to a senior leader/line manager immediately.
- Any damage or faults involving equipment or software should be reported to a senior leader.

### **Sanctions and Disciplinary Procedures**

- Any misuse of the Trust ICT systems may result in disciplinary procedures.