



CHULMLEIGH ACADEMY TRUST

ICT POLICY

Approved by Directors: Autumn 2025

Contents

1. Introduction and aims	3
2. Relevant legislation and guidance	3
3. Definitions	4
4. Unacceptable use	4
5. Staff (including directors, volunteers, and contractors)	6
6. Pupils	9
7. Parents / Carers	12
8. Data security	12
9. Protection from cyber attacks	14
10. Internet access	15
11. Monitoring and review	17
12. Related policies	17

1. Introduction and aims

ICT is an integral part of the way our schools work, and is a critical resource for pupils, staff, directors, volunteers and visitors. It supports teaching and learning, pupil support and administrative functions of the school.

However, the ICT resources and facilities our schools use 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 directors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on GDPR, 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 directors, staff, pupils, volunteers, contractors and visitors.

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 2020](#)

➤ [Searching, screening and confiscation: advice for schools](#)

3. 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 directors, 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
- **“School”**: a reference to ‘school’ means any school in the Trust, or all schools in the Trust, or the Trust, as the context requires

4. Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any member of the school community.

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
 - Online gambling, inappropriate advertising, phishing and/or financial scams
 - Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
 - Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

 - 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
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Executive Headteacher or a senior leader with delegated responsibility 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 Executive Headteacher's discretion.

Any such requests should be made in advance to the Executive Headteacher in writing with a clear explanation for the request and its expected outcome.

4.2 Sanctions

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

5. Staff (including directors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's IT Technicians and support company, IT Champion, 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 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 their Line Manager and with agreement a request can be made to the senior leader(s) with oversight of IT. Each request is considered on its own merit, examining who needs changes to their permissions and why. This will be discussed by the senior leader with responsibility for IT across the Trust alongside the Executive Headteacher/Head of School.

5.1.1 Use of phones and email

5.1.2

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

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 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 send an email in error, which contains the personal information of another person, they must inform the Executive Headteacher and Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 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 Executive 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 contact time/teaching hours/non-break time.
- 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

5.3 Remote access

The Trust allow staff to access the school's ICT facilities and materials remotely. This is managed and supported by our support company IT Champions and the IT Technicians.

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 IT Champion and IT Technicians may require from time to time against importing viruses or compromising system security.

5.4 School social media accounts

The school has an official Facebook and Twitter page, managed by the Marketing Officer/ Executive Headteacher/Head of School/delegated Senior Leaders. 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
 - › Prevent or detect crime
-

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Pupils may access the school's ICT facilities under the following circumstances.

- Computers and equipment in the school's ICT suites/classrooms are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for art/music or design and technology must only be used under the supervision of staff

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 , the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out as set out in our behaviour policy, and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or designated safeguarding lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, we will proceed according to the behaviour policy).

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Not copy, print, share, store or save the image

- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy (make sure that your searches and confiscation policy reflects the updated DfE guidance, which came into force on 1 September 2022).

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 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:

- 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
 - Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
 - 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 / Carers

7.1 Access to ICT facilities and materials

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

However, parents/carers 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 headteacher's discretion.

Where parents/carers 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 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.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

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.

We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication

➤ Anti-malware software

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.

All staff will use the password manager required by the ICT manager to help them store their passwords securely. The ICT team will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

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.

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 IT Champion/IT Technicians in consultation with the senior leader(s) with oversight of IT.

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 IT Technicians/Line 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) 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 Executive Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT Champion/IT Technicians/Senior Leader(s) with oversight of IT.

9. Protection from cyber attacks

In order to protect the Trust from cyber security threats the following measures have been implemented:

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents, which need to be reported through to the Estates Manager or Premised and ICT manager as soon as practicable. Any cyber attacks will be reviewed by the DPO and communicated through to Governing bodies such as the Department for Education, ICO etc. depending on risk score.
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
 - **Proportionate:** the school will verify this using a third-party audit at least annually, to objectively test that what it has in place is effective
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up to date:** with a system in place to monitor when the school needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be

- Back up critical data daily and store these backups on a cloud-based backup systems/external hard drives (depending on system) that aren't connected to the school network and which can be stored off the school premises. Tested recovery procedures are also available.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to IT Champions
- Make sure staff:
 - Dial into our network using a virtual private network (VPN) when working from home
 - Enable multi-factor authentication where they can, on things like school email accounts
 - Store passwords securely using a password manager
 - Password requirements are given to every member of staff when they are given a user account.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on and network security controls
- Install antivirus and anti malware software on all devices
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Encryption is in place for sensitive and personal data
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Prompt removal of access for leavers
- Access control and permissions are based on job roles and are reviewed regularly
- Account activity is monitored and audited
- Subscribe to cyber Liability insurance which provides phishing simulations, dark web monitoring, deep scanning and cyber security advice
- Undertake a cyber security audit on an annual basis, competed by an independent external party.

10. Internet access

The school's wireless internet connection is secure. Filtering is used throughout the academy. Access is only given to staff in general. Any other use is bey permission ie for use by visitors and will via a separate connection.

Staff are able to report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the relevant member of staff/service provider using the ICT helpdesk function.

10.1 Pupils

The use of WiFi by pupils is limited to the following:

- WiFi is available for specific requirements such as for specialist equipment eg blood sugar monitoring
- All wifi is filtered
- Pupils can request access via the SLT team or ICT & Premises Manager

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher or ICT and Premises Manager will only grant authorisation if:

- Parents/carers 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 WiFi 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)

Add any other circumstances where parents/carers or visitors will be granted access to the internet.

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

11. Monitoring and review

The Executive Headteacher and senior leaders with oversight for IT 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 directors are responsible for approving this policy.

12. Related policies

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

- Safeguarding & Child Protection
- Behaviour
- Conduct
- GDPR Policy
- Remote Education
- Social Media Home School Agreement
- Pupil Images Policy