Exceed Learning Partnership
• EVERY CHILD • EVERY CHANCE • EVERY DAY •

ICT Acceptable Use Policy for Staff, Directors, Governors, Visitors

Status	**Statutory**
Version	**4**
Responsible Directors' Board	**Finance and Operations Committee**
Responsible Persons	**Deputy CEO and Chief Technology Officer**
Date Policy Reviewed	**June 2026**
Next Review Date	**June 2027**
Academy to implement without Amendment, using appendix when required	

Summary of Changes from Previous Version

Version	Date	Author	Summary of Updates
V1	August 2023	Director of ICT	New Policy
V2	August 2024	Director of ICT	Updated / Amended Policy with new formatting and wording throughout.
V3	August 2025	Director of ICT	Added reference to Data Protection Policy Updated page 4 to add training categories and capture emerging technologies Updated page 6 & 7 - Title change to include 'Staff' **Communications with Parents, Pupils, Governors & Staff** Added section 8. Personal Messaging Applications Added section **Artificial Intelligence (AI) Use**
V4	June 2026	Director of ICT	Updated to reflect MFA Requirements and expectations of all staff

Contents

1. Introduction

This policy should be read in conjunction with other relevant academy and Trust policies, procedures and Codes of Conduct including:

- Social Media Policy
- ICT Policies
- Staff Code of Conduct
- Disciplinary Procedure
- Data Protection Policy

Staff should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. This includes training on online safety, data protection, and the appropriate use of emerging technologies such as Artificial Intelligence.

It is not the intention of the policy to try to police every social relationship that adults working within the academy may have with parents, directors, governors and academy staff but about reminding individuals of the importance of appropriate boundaries, including through their social media and online use.

This policy sets out clear expectations for professional conduct in the digital and online domain, acknowledging the evolving landscape of digital communication and tools.

2. Application

This policy applies to the academy local governing body, all teaching and other staff, whether employed by Exceed Learning Partnership Trust, external contractors providing services on behalf of the academy, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the academy. These individuals are collectively referred to in this policy as staff or staff members.

The policy applies in respect of all IT resources and equipment within the academy and resources that have been made available to staff for working at home. All ICT equipment issued by the organisation is monitored and managed remotely, irrespective of location, to safeguard the equipment and its use but also provide remote support.

IT resources and equipment includes computer resources, iPads/Tablets, use of academy internet access and email systems, applications and digital platforms, academy telephones and text messaging systems, web cameras and audio/video recording equipment, intranet and virtual learning environments and any other electronic or communication equipment used in the course of the employee or volunteer's work. This explicitly includes Artificial Intelligence (AI) tools, virtual meeting platforms, and all forms of digital communication channels.

This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the

expectations of staff working with children and young people.

3. Access and Expectations

1. **Login and Access Permissions**:
    - Academy staff will be provided with a unique login to access the academy ICT facilities. Staff will be informed of the specific hardware and software they are permitted to use, including internet and email access. Staff can use any available facilities unless they are currently being used by pupils or other colleagues. This access is granted to help staff perform their roles effectively and to support the wider staff community.
2. **Email Communication**:
    - Staff provided with an academy email address should use it solely for professional purposes. Communication with parents and pupils via academy email addresses is permitted under the guidelines outlines in the 'Use of Email Guidelines' policy. Staff are encouraged to use the 'Schedule Send' function to ensure emails arrive during working hours, even if drafted during personal time
3. **Software and Digital Platforms**:
    - Access to specific software packages, applications, digital platforms, online learning resources, academy texting services, and remote access is restricted to designated staff members. Unauthorised access to these systems is strictly prohibited.
4. **Digital Devices**
    - Staff will not use any technology in the Academy or throughout the Trust to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene communications, gambling and viewing pornography or other inappropriate content.
    - To maintain a professional learning environment and ensure the safety of our pupils, staff are prohibited from using personal digital devices during contact hours or at any time in the presence of pupils, except in the specific circumstances outlined below:
        - Emergency Situations: For urgent personal matters or where explicitly authorised by the Principal (for example, during off-site educational visits).
5. **Authorised Multi-Factor Authentication (MFA):**

- Staff are permitted to use personal mobile phones for the sole purpose of completing MFA requirements to access secure professional platforms, including Google Workspace for Education, CPOMS, and other work-related digital systems. When using a personal device for MFA or authorised work-related tasks, colleagues must be mindful of their surroundings and not use a personal device for MFA in the presence of pupils. It is the expectation that MFA can be undertaken at the beginning of an academy day and laptops locked so that it doesn't have to be repeated throughout the day.
    - Such use must not interfere with teaching responsibilities, pupil supervision, or the maintenance of professional boundaries.
    - This restriction applies to personal mobile phones, smartwatches, personal laptops, and any wearable technology with recording or camera capabilities

(e.g. smart glasses). Furthermore, Trust-owned equipment must not be used for personal purposes at any time.

- Staff may configure Trust email on personal devices, provided it is accessed exclusively through the official Gmail app. Upon termination of employment or departure from the Trust, users are responsible for ensuring all Trust accounts and related data are promptly removed from their personal hardware.
- Staff must keep their passwords confidential and enable Multi-Factor Authentication where available to protect the integrity of Academy data. Unauthorised access to equipment must not be permitted.
- The Trust has the right to monitor emails, Google Chat, phone calls, internet activity or document production, principally in order to avoid offensive or nuisance material and to protect systems from viruses, to ensure proper and effective use of systems. Communication systems may be accessed when the Trust suspects that the employee has been misusing systems or facilities, or for the investigation of suspected fraud or other irregularity.

6. **Storage of Documentation**:
   - All work documents, spreadsheets, presentations and other data should be saved on Google Drive unless recorded in a specific application or platform.
   - The use of USB devices for saving work is strictly prohibited to maintain security and integrity.

7. **Provision and Use of Equipment**:
   - Certain staff may receive laptops, iPads, tablets, or other equipment for their roles. Staff must ensure that these devices are password-protected and not accessible to others when used at home. Devices must not be used inappropriately by the staff member or others.

8. **ICT Equipment Maintenance**:
   - Staff must ensure that they respect and take great care of the ICT equipment they have been provided with.
   - ICT equipment must be regularly returned to work for checking and to receive updates.

9. **Recording Equipment**:
   - When using iPads or other recording devices for educational or business purposes outside the academy, staff must ensure the equipment is kept secure. Parental consent must be obtained before taking pictures of pupils, and all academy policies regarding the use of pictures must be followed. Images and videos should be periodically deleted as part of regular housekeeping to ensure privacy and security.

10. **Confidentiality**:
    - Academy staff with access to colleagues' personal contact details must keep this information confidential. Personal use of the academy telephone system is only permitted under exceptional circumstances and should occur during break periods. Any costs incurred from personal use must be reimbursed or a donation should be made towards the call costs.

4. Communication with Parents, Pupils, Directors, Governors, Staff

The Trust/Academy employs various communication methods to engage with parents, pupils, directors, governors and staff effectively.
The following outlines our authorised communication channels and protocols:

1. **Academy Telephones**:
    - All teachers, administrative staff, and staff involved in pupil welfare or home/academy liaison roles are authorised to use academy telephones for direct communication. Learning support staff should seek approval from a class teacher before making calls to parents.
2. **Text Messaging System**:
    - Office staff are primarily responsible for sending text messages. In exceptional circumstances, other staff may send texts with prior approval from the Academy Business Manager.
3. **Letters**:
    - Teachers can send letters home but may need approval from the Principal. Office staff must have letters approved by the Principal before sending.
4. **Email Communication**:
    - Academy email accounts are a primary method of communication and should be used professionally. The following guidelines apply:
        - **Parents**: Staff may use academy email accounts to communicate with parents during standard academy hours. Emails sent outside of these hours should be limited to urgent matters and require prior approval. Scheduling of emails is recommended to avoid out of hours communications.
        - **Directors and Governors**: Email is the standard communication method among academy governors, Trust directors and staff. Directors, Governors linked to specific areas or staff members may use email for direct communication without needing prior approval.
        - **Pupils**: Direct email communication with pupils is permitted only across the Secondary phase and should follow the same professionalism as communicating with colleagues. No personal contact details should be shared with pupils.
5. **Remote Communication Protocols**:
    - When communicating remotely, staff must use academy-provided systems to maintain security and privacy standards. Personal devices should not be used for

official communications without explicit authorisation.

6. **Submission of Work**:
    - Pupils submitting work electronically must use designated academy platforms, ensuring secure and traceable communication. Personal email accounts must not be used for submitting or receiving pupil work.
7. **General Guidelines**:
    - All communications should adhere to the Trust/Academy's policies on confidentiality, professionalism, and data protection.
    - Staff must regularly check and manage their academy email accounts to ensure timely responses to communications.
    - Sensitive information should be communicated securely, using encrypted email services where necessary.

8. **Personal Messaging Applications:**
    - Staff must maintain clear professional boundaries when using personal messaging apps and adhere to the Trust Code of Conduct.
    - Google Chat & Microsoft Teams are the only authorised messaging applications that may be utilised for formal conversations. Staff should be aware that this communication is also monitored in the same way web-browsing and email is monitored.

5. Social Media

Academy staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children/young people. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the academy can lead to disciplinary action, including dismissal.
Staff should refer to the Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6. Artificial Intelligence (AI) Use

The Trust recognises the potential benefits of Artificial Intelligence (AI) tools (such as Gemini, ChatGPT, and various wrapper services like "SLT AI") to enhance teaching, learning, and administrative tasks. However, their use requires careful consideration to ensure ethical practices, academic integrity, and data security.

Expectations

Staff are encouraged to explore and utilise approved AI tools to support their professional duties,

always adhering to principles of transparency, critical evaluation, and data confidentiality.

Ethical and Responsible AI Use

- **Transparency and Attribution:** When using AI tools to generate or assist in creating content for educational or administrative purposes (e.g., lesson plans, reports, communication drafts), staff should be transparent about AI's role where appropriate, especially when content is presented as authoritative or original.
- **Critical Evaluation:** AI outputs can be inaccurate, biased, or incomplete. Staff must critically evaluate any information or content generated by AI tools, cross-reference with reliable sources, and apply their professional judgement. AI is a tool for augmentation, not a replacement for human expertise.
- **Bias Awareness:** Staff should be aware that AI models can reflect biases present in their training data. Content generated by AI should be reviewed for fairness and impartiality before use.

Data Security and Confidentiality with AI Tools

- **Confidentiality:** Staff must **never** input confidential, sensitive, or personal data (e.g., pupil names, assessment data, safeguarding information, staff details, unreleased academy policies or financial data) into public AI tools (e.g., free versions of Gemini, ChatGPT). These tools may use input data for their own model training, compromising confidentiality and data protection.
- **Approved Tools:** Where the Trust provides or explicitly endorses specific AI tools or services (e.g., "SLT AI" or licensed enterprise AI solutions), these should be used in preference to public tools, as they will have appropriate data protection agreements in place. Staff must understand the data handling policies of any AI tool they use.
- **Intellectual Property:** Staff should be mindful of intellectual property rights when using AI tools, particularly if the tool uses copyrighted material for its training or generates content that might infringe on existing copyrights.

Staff must be aware that AI can 'hallucinate' (confidently state false information as fact). All AI-generated factual content or legal/safeguarding advice must be verified by a human expert

7. Unacceptable Use of Digital Technologies and Online Platforms & Systems

Academy systems and resources must not be used under any circumstances for the following purposes:

- **Confidential Information**: Communicating or sharing any confidential information related to the academy without proper authorisation.
- **Personal Views**: Presenting personal views or opinions as those of the academy, or making comments that are libellous, slanderous, false, or misrepresent others.
- **Offensive Material**: Accessing, viewing, downloading, posting, emailing, or transmitting any

pornography, sexually suggestive content, or any other offensive, obscene, or discriminatory material.

- **Defamatory Communication**: Communicating anything via ICT resources that could be considered defamatory, derogatory, discriminatory, harassing, bullying, or offensive, whether internally or externally.
- **Critical of the Academy**: Communicating anything via ICT resources that could be considered critical of the academy, its leadership, staff, or pupils.
- **Malicious Software**: Uploading, downloading, posting, emailing, transmitting, or storing material containing software viruses or any other computer code, files, or programmes designed to interrupt, damage, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment.
- **Data Protection**: Collecting or storing personal information about others without adhering to the Data Protection Act 2018 and UK GDPR.
- **Unauthorised Use**: Using the academy's facilities for trading, gambling, personal financial gain, or political purposes, unless part of an authorised curriculum project.
- **Unapproved Services**: Visiting or using any online messaging service, social networking site, chat site, web-based email, or discussion forum not supplied or authorised by the academy.
- **Safeguarding Risks**: Engaging in any activity (including communicating, accessing, viewing, sharing, uploading, or downloading) that could negatively impact the safeguarding of children and young people.

Any of the above activities are likely to be regarded as gross misconduct and may lead to dismissal after proper investigation. If employees are unsure about the use of ICT resources, including email and the intranet, they should seek advice from a member of the Senior Leadership Team or the ICT lead.

If an individual accidentally accesses a website or material they consider pornographic or offensive, this must be reported immediately to the Designated Safeguarding Lead (DSL). The academy's filtering and monitoring systems should block such content, but reporting applies even if the incident occurs using academy equipment at home. Genuine mistakes and accidents will not be treated as a breach of this policy.

If an individual receives inappropriate communication (e.g., an email or attachment), they should report it immediately to the DSL and ICT Support Team for appropriate action.

8. Security and Confidentiality

Any concerns about the security of the ICT system should be raised with the Principal and/or the Chief Technology Officer.

Staff are required to:

- **Password Management**: Keep all passwords confidential, avoid easily guessed passwords, and regularly change them when requested to do so. Multi-Factor Authentication (MFA) must be

enabled and utilised for Google Workspace, CPOMS, and other work-related systems to ensure robust protection of sensitive data.

- **Downloading Material**: Follow guidelines issued on downloading educational and professional material to Google Drive. Only download material from known and reputable sites to maintain system integrity. Report any issues encountered during downloading to the DSL or ICT Support Team.
- **Working Remotely**: Ensure the use of personal systems is limited. Where use is required, appropriate virus-detection software should be installed and care should be taken when working on material at home and uploading it to Google Drive.
- **Approval Processes**: Adhere to approved processes before uploading any material for pupil use on the pupil ICT system and/or VLE. Additionally, any material for the academy website must follow the agreed approval processes.
- **Virus or Malicious Activity Concerns**: Notify the Principal / ICT Support Team of any concerns regarding potential viruses.
- **Data Protection**: Ensure that their use of the academy's ICT facilities does not compromise individual rights under the Data Protection Act 2018 and UK GDPR.

To maintain data security and confidentiality, staff must also be aware of and adhere to the following practices:

1. **USB Drives are prohibited**:
    - Use Google Drive for storing and sharing documents instead of USB drives to prevent data breaches and data loss.
2. **Email Security**:
    - Do not click on links or reply to emails from unknown or suspicious sources to avoid phishing attacks and malware.
    - Verify the correct email address and the identity of the recipient before sending personal data.
3. **Data Sharing**:
    - Avoid over-sharing data. Only share information that is necessary and ensure it is done through secure channels.
    - Limit access to sensitive information to only those who need it for their role.
4. **Printing Data**:
    - Print documents only when absolutely necessary. Securely store or dispose of printed documents to prevent unauthorised access.

5. **Secure Storage**:
    - Store electronic data securely in authorised data storage locations (Google Drive).
    - Keep physical documents in locked cabinets or secure areas.
    - Do not use USB or External Hard drives for storing or transporting data.
6. **Internet Use**:
    - Do not visit unapproved websites or use personal social media during working hours to maintain productivity and security.

7. **Device Security**:
    - Ensure that personal devices used for work are secure and free from inappropriate content.
    - Prevent pupils from accessing staff personal devices at any time.
8. **Reporting Incidents**:
    - Report any security incidents, breaches, or suspicious activities immediately to the DSL or the ICT department.

The Trust ICT Support Team is responsible for ensuring all equipment is regularly updated with new software, including anti-virus and anti-malware packages, and maintaining software licenses for all academy-based and academy-issued equipment.

Staff must ensure their use of the academy's ICT facilities does not compromise individual rights under the Data Protection Act 2018 and UK GDPR.

By adhering to these guidelines, staff can ensure the security and confidentiality of the academy's ICT systems and protect the integrity and privacy of data.

9. Equipment Monitoring & Reporting

The Trust ICT Support Team use several remote monitoring, filtering and reporting applications to keep the ICT equipment owned by the Trust/Academy safe, secure and stable. These systems are in place to ensure compliance with DfE guidance on filtering and monitoring and to safeguard all users.

The Trust reserves the right to monitor the use of email, internet access and other digital communication channels, and where necessary this data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the academy and Trust hardware, software, networks and systems are not compromised
- to prevent or detect crime or unauthorised use of the Trust or Academy hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent from work
- in the event of a subject access request

Where staff have access to the internet on organisation issued devices, it is important for them to be aware that the academy will monitor and track the history of the internet sites that have been visited.

To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Deputy CEO / CEO , after

discussions with relevant staff and following an assessment to determine whether access or interception is justified.

10. Security Controls

To safeguard our systems from the risks posed by viruses and malware, the following measures will be implemented:

- Anti-Malware Software: Will be installed, maintained and configured to routinely scan on all devices.
- Regular Updates: Operating systems and all software applications patched with the latest updates to protect against vulnerabilities.
- Phishing Protection: Phishing filters will be enabled on web browsers to reduce the risk of phishing attacks.

Any devices identified or suspected to be infected must not be used to access the academy's network. The device will be inspected by the Trust ICT Support Team and the correct course of action applied.

Data security:

To avoid a risk of confidential information being disclosed to unauthorised third parties all staff should:

- Lock or logout of their devices or remote access before leaving their computer.
- Do not allow any unauthorised person, including family and friends, to use their work issue devices.
- Never reveal or share passwords. If for any reason a password is revealed/shared this should be changed immediately.
- Exercise caution when viewing sensitive information in public places (Train, Bus, Coffee Shops) where it may be possible for data to be seen over your shoulder.

11. Whistleblowing and Cyber Bullying

Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the DSL, Principal or Chief Technology Officer to such abuse.

Where a concern relates to the Principal, this should be disclosed to the CEO or Deputy CEO. If any matter concerns child safety, it should also be reported to the Head of Safeguarding.

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of academy staff. Staff are strongly advised to notify their Principal where they are subject to such

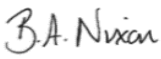
circumstances.

Advice can also be sought from professional associations and trade unions.

Further advice on cyberbullying and harassment can be found in the Academy Social Media Policy and in the Online Safety and Security Policy .

In addition to this, colleagues throughout the Trust are trained to log concerns onto CPOMs in a professional and appropriate way.

Policy Reviewed June 2026

Signed Chief Executive: 

Signed: Chair of Directors: 

Policy to be reviewed in June 2027