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

ICT Acceptable Use Policy, Staff, Governors and Visitors

Author/Owner (Name and Title)	Safeguarding Lead
Version Number	New Policy
Date Approved/Reviewed	September 2023
Date of Next Review	September 2024
Approved By	Full Board of Directors

Policy Category (Please Indicate)	1	**Academy to implement without amendment**
	2	Academy specific appendices
	3	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Summary of Updates
V1	New Policy		

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
- Code of Conduct
- Disciplinary Procedure

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.

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, governors and academy staff but about reminding individuals of the importance of appropriate boundaries, including through their social media use.

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. IT resources and equipment includes computer resources, Ipads, use of academy internet access and email systems, software (including use of software such as SIMS, online applications OTrack, Twitter, Seesaw, Tapestry), academy telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work. 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

Academy staff will be provided with a login where they are entitled to use the academy IT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the academy to benefit from such facilities. Where staff have been provided with an academy email address to enable them to perform their role effectively, it will not be used to communicate with parents and pupils. Where staff are able to access emails outside of academy hours, the email facility will not routinely be used to email parents outside of normal academy hours.

Access to certain software packages and systems (SIMS, FMS, Perspective, OTrack, Seesaw, Tapestry, MyPE, Reading eggs, TT Rockstars, Mathletics, RWInc spelling, Reading Plus) and other online learning resources, academy texting services and remote access will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops or Ipads and other equipment for the performance of their role. Where provided, staff must ensure that their academy laptop/other equipment is password protected and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection. Any documents created and saved must be on one drive and not on a USB device without security password encryption.

Where the academy provides IPads and other recording equipment for educational and academy business use and it is used away from the academy site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the academy's policy in relation to use of pictures, is followed and these are deleted once used for display/ Twitter.

If the academy does not provide academy mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the academy will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the academy rather than a direct call from the individual's personal mobile. Academy staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

Whether academy staff have access to the academy telephone system for personal use will be confirmed by the academy for exceptional circumstances. Where such use is made of this facility, it must be done during break periods, must not be excessive and the academy should require either the cost of the call or a donation to be made towards the cost of the call.

The academy will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4. Communication With Parents, Pupils and Governors

The academy communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. Academy must indicate to staff if any other staff are permitted to make contact using the systems below:

Academy Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/academy link staff. Normally learning support staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by the Academy Business Manager

Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Principal before sending. Where office staff send letters home these will normally require approval by the Principal.

Email – academy email accounts will not routinely be used for communication with parents outside academy hours.

Email is used as a normal method of communication amongst academy governors and where governors are linked in particular areas with members of staff, communication may take place via email.

Under normal circumstances, academy staff will not be using any of the methods outlined above to communicate directly with pupils.

Where pupils are submitting work electronically to academy staff, this must be undertaken using academy systems and not via personal email.

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 Academy Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6. Unacceptable Use

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

- to communicate any information that is confidential to the academy or to communicate/share confidential information which the member of staff does not have authority to share
- to present any personal views and opinions as the views of the academy, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally
- to communicate anything via ICT resources and systems or post that may be regarded as critical of the academy, the leadership of the academy, the academy's staff or its pupils

- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment
- to collect or store personal information about others without direct reference to The Data Protection Act
- to use the academy's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project
- to use the academy's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the academy
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

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

Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Designated Safeguarding Lead (DSL). The academy's filtering and monitoring systems should provide appropriate blocking software to avoid the potential for this to happen. Reporting to the DSL equally applies where academy staff are using academy equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the DSL so that this can be dealt with appropriately.

7. Personal and Private Use

All academy staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the academy
- detrimental to the education or welfare of pupils at the academy

Excessive personal use of academy facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the academy will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

Where academy staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the academy, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any academy data/images are deleted following use of the equipment.

Whilst individuals may be required to use their personal mobile telephone to make contact with the academy, staff should exercise care and seek reimbursement as outlined in section 3.

8. Security and Cofidentiality

Any concerns about the security of the ICT system should be raised with the DSL.

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

Academy staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the academy server. Where staff are provided with a memory stick for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the academy's systems. Where problems are encountered in downloading material, this should be reported to the DSL.

Where staff are permitted to work on material at home and bring it in to upload to the academy server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

Whilst any members of academy staff may be involved in drafting material for the academy website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

The Trust approved provider is responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all academy based and academy issued equipment. Staff must ensure that they notify the DSL when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the academy's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

9. Monitoring

The academy uses the Trust approved provider for ICT monitoring.

The academy and Trust reserve the right to monitor the use of email, internet and intranet communications and where necessary 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 academy or Trust hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the academy may 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 Chief Operations Officer, after discussions with relevant staff and following an assessment to determine whether access or interception is justified.

10. Whistleblowing and Cyberbullying

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 to such abuse. Where a concern relates to the Principal, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

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 'Cyber bullying: Practical Advice for Academy Staff' section of the ICT Policy.

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

11. Remote Access Policy

The academy provides remote access to the Principal, Deputy Principal, Academy Business Manager and Office Manager. Use of the academy's remote access service implies acceptance of the conditions of use. The academy may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

Uses of Remote Access Services

The following list is not exhaustive, but sets out broad areas which the academy considers to be acceptable use of remote access.

- To gain access to Academy Information Management System (SIMS)
- To gain access to resources, files and software on the academy network
- To administer the academy network remotely

Use of Computers and Equipment

Any computer used to access the academy's remote systems must possess anti-virus and anti-spyware programs. These must be updated regularly, at least once a week. The academy bears no responsibility if use of the remote access system causes system crashes, or complete or partial data loss on connected computers. Users of remote access are solely responsible for backing up all data before accessing the system. At its discretion, the academy will disallow remote access for any computer that proves incapable, for any reason, of working correctly with the remote access system.

Potential Security Issues

Viruses and malware:

When a computer is directly connected to the internet it can be contacted by any other computer also connected to the internet. As a result, there is a risk of exposure to malware that could connect to and potentially compromise that computer, which in turn risks infecting the academy's system. For this reason, precautions must be taken to minimise this risk:

- Make sure up-to-date anti-virus software is installed.
- Make sure the latest operating system patches are installed.
- Run a weekly virus scan.
- If a computer has become infected with a virus or other malware, do not use it to remotely access the academy's network until the virus has been deleted.
- Turn on phishing filters on web browsers to reduce the risk of phishing attacks.
- Use an anti-spyware program to detect spyware.

Data security:

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

- Logout of remote access before leaving the computer.
- Wireless network connections must be encrypted using WPA2 or use a cable connection.
- Do not allow any unauthorised person, including family and friends, to use the remote access login or to access files held on the academy's network.
- Use a password protected screensaver to prevent anyone gaining access to the computer
- Do not use password storing facilities found in some programs to automatically remember passwords.
- Do not reveal passwords. If for any reason a password is revealed this should be changed immediately.

This policy will ensure that staff are able to access the academy network remotely without risk to the security of the system.

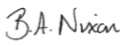
It will be normal practice for staff to read and sign a declaration, to confirm that they have had access to the Acceptable Use Policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

Date of Policy Approved September 2023

To be reviewed September 2024

Beryce Nixon

CEO Signature: 

John Blount

Chair of Directors Signature: