MacIntyre Academies

Acceptable use of Information, Communication Technology Policy

Version	Updates / Changes	Responsibility	Date
V6	2 Updated to reflect latest versions of regulation and statutory guidance. 5.4 Sentence added to reflect that emails sent to and from Trust email accounts are the intellectual property of the Trust. Added reference to the Code of Conduct. 5.8.1 Updated that permission to access the Wi-Fi at an Academy be granted by the Principal / Head of Care / Head of Operations 5.9 Updated to reflect current practice 6.1 Updated that on Trust devices passwords may be saved to browsers, where users adhere to this policy 7. Added Trust participation in Policy Cyber Alarm scheme 7. Updated detail around Cyber Security training 9. Added, school mobile phones may be used to take photographs of pupils 10. Removed paragraphs relating to Safeguarding and referred instead to Academy Safeguarding Policies. Appendix 1 – update to point D.	Head of Operations	Sep 23

Person Responsible:	Head of Operations
Date of first draft:	September 2016
Date of staff consultation:	November 2016
Date adopted by the Trust Board:	06/12/2016
Date of implementation:	December 2016
Date reviewed:	September 2023
Date of next review:	September 2025

==Contents

1. Introduction

Information and communications technology (ICT) is an integral function facilitating the work of the Trust and its academies and must be used to best serve our vision across all of our provisions - *for all young people to have confidence and belief in their potential, be ready for a successful adult life and connected where they live.*

Our aim is to ensure that staff and volunteers and, where relevant, agency workers, have good access to digital technology to enhance their work and therefore enhance learning opportunities for children and young people (CYP). In return our expectation is that staff, volunteers, and agency workers agree to be responsible users and adopt good user habits which will enhance security.

We have a proactive approach to defending our ICT systems and facilities from cyber-threats. Our staff undertake annual Cyber-security Awareness Training as well as receiving regular emails and alerts as relevant throughout the academic year. Our systems are subject to routine testing, and we keep pace with sector wide trends as threats evolve and change.

Our aim is to provide a user-friendly policy and procedure to ensure users across the academies can operate efficiently, maximising the benefits of ICT, whilst critically also ensuring the safety of our systems and information.

All staff, agency workers and regular volunteers, including those involved in our governance, are required to read, and sign the 'Acceptable Use of Technologies' agreement during their induction and at every review.

This policy aims to:

- Set guidelines and rules on the safe use of ICT resources for all users
- Establish clear expectations for the way users engage with each other online
- Support the MAT Data Protection Policy, the Academy Online Policies (or E-Safety Policy) and the Academy Safeguarding Policies.
- Prevent disruption to the Trust and its academies through the misuse, or attempted misuse, of ICT systems
- Support the academies in teaching CYP safe and effective internet and ICT use

This policy applies to all 'users' of our ICT, being:

- employees of MacIntyre Academies Trust
- supply/agency staff
- volunteers and visitors
- contractors
- those with a role in our governance

This policy applies where ICT is used at one of our academies and where ICT is used remotely from any location.

Breaches of this policy may be dealt with using the MAT Disciplinary Policy.

This policy does not form part of any contract of employment and will be reviewed regularly and amended as required.

2. Relevant legislation and guidance

This policy is written in accordance with:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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 2023
- Searching, screening and confiscation: advice for schools
- Meeting digital and technology standards in schools and colleges
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021
- UK Council for Internet Safety (et al.) guidance on Sharing nudes and semi-nudes: advice for education settings working with children and young people

3. Definitions

ICT (information and communications technology): This is an umbrella term that includes any communication device or application, encompassing: cameras, mobile phones, smart watches, computer and network hardware and software, satellite systems etc., and the services and applications associated with them e.g. videoconferences, e-learning, databases, and electronic records.

ICT includes technology that can be used to store, transmit or manipulate data, such as MP3 players, Personal Digital Assistants (PDAs) and USB media, including any device that can connect to the internet.

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 Trust or its academies to use the ICT facilities, including governors, staff, agency workers, volunteers, contractors, and visitors

Cyber-security: the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Personal use: Any use or activity not directly related to the users' employment, study, or purpose

Authorised personnel: Employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities

Materials: Files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Responsibilities

MacIntyre Academies Trust Board

Have strategic responsibility for ratifying this policy, ensuring that it is reviewed every two years or earlier where required.

Have strategic oversight of the Trusts defences against cyber-attack and take appropriate action where a cyber-attack occurs.

Local Advisory Board

Monitor and evaluate the effectiveness of the policy and practice, in line with the Scheme of Delegation and LAB Terms of Reference.

Group Director

Hold Principals, Head of Care and Head of Operations to account for the implementation of this policy. Have strategic responsibility for the Trusts defences against cyber-attack and take appropriate action where a cyber-attack occurs.

Head of Operations

Manage the ICT contract and take responsibility for the review and implementation of this policy at a Trust wide level. Have strategic responsibility for the Trusts defences against cyber-attack and take appropriate action where a cyber-attack occurs.

Academy Principals and Head of Care at Endeavour House

- Ensure all users, being staff, volunteers and/or students on work placements as defined in Section 1 are familiar with and have access to a copy of this policy.
- Ensure all users sign the Acceptable Use Agreement (Appendix 1) as part of induction and when there has been a significant change.
- Ensure staff and volunteers comply with this policy and procedures.
- Ensure cyber security and best practice is held in appropriate regard in their academy culture
- Ensure their academy have an E-Safety Policy which includes the storage and transmission of personal data, and robust procedure for the 'Use of mobile phone and camera technologies'.
- Ensure that MAT approved software is used for transmitting all sensitive data.

All Users (including staff, agency workers, volunteers, and pupils on placement/work experience) must:

- Abide by this policy
- Promptly report suspicion or occurrence of any unauthorised activities.
- Complete all mandated training within the timescales requested
- Sign the Acceptable Use Agreement (Appendix 1) on induction, and at the point of any review with significant updates.

5. General Use

Users must treat equipment and services with respect, and are subject to regulations imposed by the respective service providers as well as by this policy.

Users must communicate online in a professional manner and tone (this includes communication by text message) and will not use aggressive or inappropriate language nor compromise either the Academy or the Trust's reputation; with an awareness that all communication can be accessed by the Trust and/or forwarded onto our network provider so that they might access it.

5.1 Un-acceptable use of ICT:

a) Using our ICT equipment for personal matters beyond what is defined in section 5.7.
b) Using personal devices or ICT equipment for Trust or Academy matters (unless sanctioned by a line manager).
c) Using our ICT facilities to breach intellectual property rights or copyright. Anyone found to have unauthorised copies of software will be investigated and the necessary action taken, the Trust will not accept liability.
d) Using our ICT facilities to bully or harass someone else, or to promote unlawful discrimination
e) Breaching any Trust or Academy policy or procedure
f) Any illegal conduct, or transmission of statements which are deemed to be advocating illegal activity
g) Online gambling, inappropriate advertising, phishing and/or financial scams
h) Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate or harmful
i) Consensual and non-consensual sharing of nude and/or semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
j) Activity which defames or disparages the Academy, or Trust or risks bringing either into disrepute
k) Sharing confidential information about the Academy, its pupils, or other members of the Trust's community
l) Connecting any device to the ICT network without approval from authorised personnel
m) Setting up any software, applications, or web services on the 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
n) Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
o) Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the ICT facilities
p) Causing intentional damage to the ICT facilities
q) Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel
r) 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
s) Using inappropriate or offensive language
t) Promoting a private business, unless that business is directly related to the Trust
u) Using websites or mechanisms to bypass the Trust's filtering mechanisms
v) Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way
w) Install non-approved content onto the settings computer/laptops, or alter laptop or computer settings or open up pop ups or attachments from untrusted sources.
x) Attempt to use any form of hacking/cracking software or system. "Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the Trust network will be prosecuted.

y) Users must agree to comply with all software license agreements and must not attempt to copy any software from, or by using Trust computers.
z) Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the General Data Protection Regulations 2018.
aa) Users should not send or receive personal emails or phone calls when on Trust premises during working hours, or use chat and social networking sites, unless otherwise agreed by the Academy Principal (or the Head of Care / Head of Operations). *Note that this is acceptable when taking breaks from work providing that young people are not present.*

This is not an exhaustive list. Senior Leadership within MacIntyre Academies will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

Users are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990).

The Trust reserves the right to monitor all usage of ICT equipment by its employees, including but not limited to emails sent and received and internet history (more detail in Section 5.9).

5.2 Conduct Outside of Work ICT

- Users must not engage in any on-line activity that may compromise their professional responsibilities or compromise the reputation of the setting or the safety and well-being of the children or staff. Staff members must ensure their online persona should be in keeping with their professional status.
- Users are advised to keep a professional relationship with CYP, parents and managers and must not befriend them on chat or social networking sites. Any pre-existing friendships or connections must be declared via a conflict-of-interest disclosure.
- Users are advised not to post any photos of themselves at work, or any photos of children and young people on their social networks.
- Users are required to check their online activity to ensure no unauthorised activity has occurred. If unauthorised activity is discovered staff must inform their line manager without delay so this breach in their security can be logged.

5.3 Access to ICT facilities and materials

The School Business Manager (or the Head of Operations for the MAT Central team) manages access to ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets, mobile phones, and other devices
- Access permissions for the network according to their role

Users who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the School Business Manager without delay.
Users will be provided with unique log-in details that they must use when accessing ICT facilities. Users must set up two factor authentication to secure their account.

5.4 Emails

The Trust provides each member of staff (and sometimes volunteers or agency workers) with an email address which should be used for work purposes only.
Users must understand that emails to and from their work account are the intellectual property of MacIntyre Academies and must not be forwarded or sent to personal email accounts unless the email relates only to them personally as a user (such as their Payslip, Contract, or other direct correspondence).

Users must not share their personal email addresses with parents/carers and CYP, and must not send any work-related materials using their personal email account.
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.

- Users 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.
- E-mail attachments from unknown senders must not be opened. Suspicious emails must be reported via the IT helpdesk.
- Users must not send e-mail messages in 'the heat of the moment' and must avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude, or offensive. Refer to point 27.3 of the Code of Conduct.
- Users must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted and sent using the MAT agreed software (EGRESS) so that the information is only accessible by the intended recipient.
- If a user receives an email in error, they should inform the sender and deleted the email. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If users send an email in error that contains the personal information of another person, they must follow the procedure in the MAT Data Protection Policy immediately. Where staff are in any doubt about the procedure, they should seek advice from the School Business Manager or a member of the Senior Leadership Team without delay. (in the case of MAT Central staff, the Head of Operations).

5.5 Networks and Files

- Staff must use Office365 to store files, and avoid saving files on the local hard drive. This will ensure that work is backed up and can be retrieved in the event of a hardware failure or theft.
- In the exceptional case where there is justification of use of a memory stick or external hard drive, this must be a Trust issued encrypted device.
- Staff should ensure that old unused files are deleted when no longer required. Refer to the MAT Data Retention Schedule for timescales for archiving key documents.
- Users accessing software or any services available through Trust facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- All staff will only transport, hold, disclose or share personal information about themselves or others where necessary and appropriate, and in ways agreed by their line manager. For more information about the handling of personal data see the MAT Data Protection Policy.

5.6 Remote access

Office365 facilitates remote access to the system. Staff accessing the Trust'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 Trust's ICT facilities outside the Trust and take such precautions as the Trust may require from time to time against importing viruses or compromising system security.
Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the MAT Data Protection Policy.

5.7 Personal use

Staff are not permitted to use Trust ICT facilities for personal use without prior express permission from their Line Manager. This is subject to certain conditions as set out below:

- Does not take place during working hours
- Does not constitute 'unacceptable use', as defined in section 5.1
- Takes place when no CYP are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (section 5.9). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the MAT Social Media Policy and use of email (section 5.4) to protect themselves online and avoid compromising their professional integrity.

5.8 Use of privately-owned devices including mobile phones

5.8.1 Use of non-Trust devices at an academy:

Personal laptops and/or other personal devices including mobile phones and smart watches are not allowed to be connected to the Trust network (namely Wi-fi in academies) unless permission is obtained from the Academy Principal (or Head of Care), where permission has been given, they must only access the Guest network.

Staff should only use their personal mobile phones or smart watches at appropriate times of the day e.g. break times, before/after normal working hours, providing pupils are not around. During the school day their personal mobiles should be turned off or set to silent, and locked away e.g. in a locker, as per the academy's 'Use of mobile phone and camera technologies' procedure.

Where an exceptional circumstance causes a member of staff to ask for permission to keep their mobile phone with them while at work, this must be with the written agreement of the Principal. The Principal must be able to give an account for why the exception has been made and keep the decision under regular review.

Staff must not use personal mobile devices or cameras to take images of children or staff.

5.8.2 Accessing emails and other resources via Office365 from a non-Trust device:

Staff may from time to time need to access emails using Office365 from a non-Trust device. This is acceptable where there is justification and adequate time taken to ensure the security is sufficient and that doing so does not represent a security risk to the system or the data.

- Where the device uses antivirus software, this must be up to date and provide adequate protection against virus'
- Where the device uses Apps to access Office365, the user must have the app set up to require the password at every point of access
- Where systems are accessed, they should be logged off after use without delay
- Care must be taken that documents are not downloaded onto any device used to access them.

5.8.3 Systems which must not be accessed from a non-Trust device

Web-based systems such as HR, Payroll and Finance system logins must never be accessed from non-Trust devices.

5.9 Trust / Academy social media accounts

The Trust has an official Twitter page, which is the responsibility of the Head of Operations. Each Academy has an official Twitter page which is the responsibility of the Academy Principal. Various members of staff will be given delegated responsibility to manage these, however, staff members who have not been authorised to manage, or post to, the account must not access, or attempt to access these accounts.

5.10 Monitoring of Network and use of ICT facilities by all

The Trust ensures that effective systems are in place to monitor and filter the activity on the Trust networks. The monitoring of activity occurs at different levels for different users.
The Trust reserves the right to monitor the use of its ICT facilities and network by all users. This includes, but is not limited to, monitoring of:

- Internet browsing history
- 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 Trust monitors ICT use in order to:

1. Comply with Keeping Children Safe in Education, and Safeguard children and young people
2. Obtain information related to Trust/Academies
3. Investigate compliance with policies, procedures, and standards
4. Ensure effective academy and ICT operation
5. Conduct training or quality control exercises
6. Prevent or detect crime
7. Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Data Security

6.1 Passwords
Users must use strong passwords

A strong password must:

1. Be long (8 or more characters)
2. Include a range of characters, such as:
   - Upper case and lower-case letters
   - Numbers
   - Punctuation marks
   - Other symbols
3. Not contain single dictionary words, where possible. Note that phrases or two words together is better.
4. Not include simple substitutions of characters, e.g. "p4$$w0rd"
5. Not include patterns derived from the keyboard layout, e.g. "qwerty"
6. Not use obvious choices of passwords, such as the name of your child or pet, as someone could find such information elsewhere.

Saving passwords in browsers on Trust devices: Passwords may be saved directly into a Trust device browser under the following conditions.

- The device is always securely protected. This means following this policy and in particular ensuring that a login is not left unlocked when unattended.
- The browser is not synchronized with any personal email account, which could inadvertently synchronize work passwords on personal devices.

Saving passwords in browsers has been allowed in order to support the use of strong passwords and avoid the need for written records of these.

Passwords must never be saved to browsers on non-Trust devices

Users must not share passwords: Password sharing for systems that protect personal data is not allowed. Sharing accounts, or even occasional use by anyone other than the account holder, negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost.

Changing passwords: Users will be prompted periodically to change their password. Passwords must be strong as detailed above.
Users also need to change their password if there is any reason to believe their password may have been compromised.

6.2 Software updates, firewalls, and anti-virus software

All of our 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 in place but abide by and maintain them to protect personal data and the Trust's ICT facilities.

Users must regularly restart their laptops (best practice being to do so at the end of every working day) in order to ensure updates are completed at the intended times.

6.3 Encryption

The Trust ensures that its devices and systems have an appropriate level of encryption.

7. Protection from **Cyber-attacks**

The Trust will:

- Work with the Trust Board and the ITC provider to ensure cyber security is given the time and resources it needs to ensure security
- Participate in the Department for Education's Police Cyber Alarm programme.
- Ensure staff undertake the National Cyber Security Centre training on cyber security in schools (and include relevant updates in training throughout the academic year, ensuring that Cyber Security is in the fore front.
- Make sure staff are aware of the procedures for reporting and responding to cyber security incidents
- 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 Trust will verify this using a third-party audit regularly to objectively test that what it has in place is up to scratch
    - **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 Trust needs to update its software

- **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

- Back up critical data daily and store these backups on cloud-based backup systems that aren't connected to the network.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT provider, with oversight from the Head of Operations.
- Ensure users enable multi-factor authentication
- Ensure ICT staff conduct regular access reviews to check all users have the correct level of permissions/ admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the ICT provider, for example, including how the Trust will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

Users must work with an awareness of potential cyber-attacks.
Emails with unexpected attachments or links must be considered with suspicion and great care must be taken.

8. Procedure for reporting ICT issues

8.1 How to report general ICT issues

For day-to-day ICT difficulties such as local hardware issues, syncing difficulties, email access, users should:

1. Speak with their line manager who will discuss the issue and identify the best course of action.
2. Where support from the ICT helpdesk is identified as the best course of action raise a ticket by emailing:
   helpdesk@flywheel-it.co.uk
   or raising a ticket online at:
   https://flywheel-it.co.uk/support/

8.2 How to report a potential cyber attack

Whilst the aim of our training is to ensure all users navigate ICT systems with due caution, we recognise that human error can occur and encourage users to have a proactive approach to reporting potential security breaches:

If a user is concerned there may have been a security breach, they should follow the steps below:

1. Disconnect the device from the internet connection and close all applications
2. **Call** the ICT provider Helpdesk:
   - Normal business hours: 01248675800 / 02039 858585
   - Out of hours: 02039 858585

   The ICT provider will triage the concern and determine any immediate action required.
3. Follow any recommendation from the ICT provider
4. Contact your line manager to update them regarding the occurrence

9. Off-site child data

- Staff must ensure that the personal data for any child or family is kept private and confidential, except when we are required by law or by the setting's policy to disclose it to an appropriate authority.
- Images of children may be taken to evidence learning progress, academies will ensure that parent/staff permission is obtained before the images are taken.
- Staff must only use school mobile phones, cameras, I-Pads, tablets, and video equipment to take images of children or staff. Images may be taken on or off-site.
- Data, images, and child information must be removed from devices, back-ups, and laptops (including 'trash') and transferred to the school network as soon as possible, but within 3 school days.
- Videoconferencing and Webcams should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.
- The use of the names of children or photographs of children for websites will require written permission from parent(s)/carer(s) included on the consent form. If a picture is placed on the website, it will be done by an authorised person. The child's name will not be displayed, and any associated information will not hold any possibility of any child featured to be identified or to find any other personal information about them.
- Staff are to ensure that laptops are used cautiously when viewing child data/information and images and that laptops are logged off when left unattended.

10. Safeguarding

Safeguarding is the responsibility of all users. Refer to the Academy Safeguarding Policy.

11. Disciplinary Procedures

If staff break the rules as laid down by this policy, they may lose temporary or permanent use of the Trust systems and will be subject to disciplinary proceedings.

If the law has been broken the police will be informed and the school will assist the police with any prosecution.

12. Additional Information

When staff leave MacIntyre Academies Trust their user account and any associated files, email address and any associated emails are removed from the ICT system and will no longer be accessible. In the case of long-term absences e.g. sick leave or maternity leave, accounts will be suspended.

13. Monitoring Compliance and Impact

We will review this policy at least once every two years, or following an incident that suggests the need for review.

Appendices:

1. **Staff (and Volunteer) Acceptable Use Policy Agreement**
2. **Permission for Personal Use of MacIntyre Academies ICT**

Appendix 1

Staff (and Volunteer) Acceptable Use Policy Agreement

I will use the Trust ICT facilities and systems in a responsible way with due regard for cyber security and data protection.

For my professional and personal safety:

a) I have read and will abide by this Acceptable Use of ICT Policy.

b) I understand that my use of the Trust's digital technology and communications systems will be monitored.

c) I understand that this policy relates to my use of the Trust's digital technology and communications systems at academies and also when I use/access these from any remote location.

d) I will not use the Trust systems for personal or recreational use unless this has been approved using the *Permission for Personal Use of MacIntyre Academies ICT Form* (Appendix 2)

e) I will use secure passwords in line with this policy. I will not disclose my passwords to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

f) I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school / academy ICT systems:

g) I will communicate with others in a professional manner, I will not use aggressive or inappropriate language.

h) I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of Mobile Phone and Camera Technologies.

i) I will not use my personal equipment to take or record images or videos.

j) Where these images are published (e.g. on the school website/ social networks) it will not be possible to identify by name, or other personal information, those who are featured.

k) I will **only** communicate with children and young people and their families/ carers using official school systems. Any such communication will be professional in tone and manner.

l) I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy or Children's Home:

m) I will undertake all training as required by the Trust in the required time frames.

n) I will be vigilant and have due caution with emails. I will not open links in emails or any attachments to emails, unless the source is known and trusted.

o) I will seek permission before connecting any personal devices to the school network, and link only using the Guest login.

p) I will not use personal email addresses on the academy ICT systems, unless permission has been given by the Principal (or Head of Care / Head of Operations).

q) I will ensure that my devices are kept up to date (regularly re-starting and running updates).

r) I will only transport, hold, disclose or share personal information about myself or others, as outlined in the MAT Data Protection Policy.

s) I understand that the MAT Data Protection Policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.

t) I will immediately report any damage or faults involving equipment or software; however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school / academy:

- I understand that this Acceptable Use of ICT Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment remotely and my use of personal equipment on the premises or in situations related to my employment by the Trust.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trust Board and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use Trust digital technology systems (both in and out of school) and on my own devices (in school and when carrying out communications related to the Trust) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date:

APPENDIX 2

Permission for Personal Use of MacIntyre Academies ICT

This form should be used to record where permission has been granted for Personal Use and define the use that has been agreed.

Employee name and role:	
Academy:	
Line manager name and role:	
Date of request:	
Type of agreement (please delete)	One off occasion / Ongoing permission
Date permission will cease (if applicable)	
Device which will be used for Personal Use:	
Use(s) permitted: *E.g. Use for a governor role at another school.* *E.g. Use for CPD pursued and paid for privately*	

Personal use of ICT, where permission has been granted is only acceptable when the following applies:

- Does not take place during working hours
- Does not constitute 'unacceptable use', as defined in section 5.1
- Takes place when no CYP are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (section 5.9). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the MAT Social Media Policy and use of email (section 5.4) to protect themselves online and avoid compromising their professional integrity.

School Business Manager / Head of Support Services name and signature:		Date:	
Employee signature:		Date:	