MOUNTVIEW

IT ACCEPTABLE USAGE POLICY

Contents

1. INTRODUCTION

1.1 BACKGROUND

Information Technology (IT) at Mountview includes the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.

Mountview has a responsibility to protect company data, systems and devices against unauthorised access and modification. All users of Mountview's IT systems, facilities and networks must do so within the law, and within the terms set out by the Academy.

1.2 PURPOSE

The purpose of the IT Acceptable Usage Policy is a formal statement to outline the acceptable and responsible use of Mountview's IT resources and network. This policy aims to protect the integrity, safety and security of Mountview's IT and data infrastructure while supporting the academic and administrative functions of the academy.

1.3 SCOPE

This policy applies to any user who accesses Mountview's IT services, including (but not limited to):

- The use of Mountview owned hardware, regardless of user location, including but not limited to desktop, laptop, tablet and Mac computers, smartphones, mobile networking devices and storage drives.
- The use of Mountview owned software and applications, regardless of user location, including but not limited to email, on premises and cloud storage, databases and 3rd party software providers.
- Mountview's network facilities, wired and wireless, whether accessed using Mountview devices or through the use of authorised personal devices.

This policy applies to ('Users'):

- All full-time, part-time, freelance, sessional and temporary staff employed by or working on behalf of the Academy.
- All students studying at the Academy.
- All Board members of the Academy.
- Contractors and consultants working for or on behalf of the Academy.
- All authorised visiting individuals or groups who have been granted access to Mountview's systems and networks by the Academy.

It is the personal responsibility of each individual user to adhere fully with this policy's requirements. In addition, it is the duty of Line Managers and Programme Leaders to implement this policy within their departments and to oversee compliance by staff and students under their direction.

As soon as a user ceases to satisfy the criteria set out above, they lose the right to access and use Mountview's IT and networking facilities.

2. LAWS, REGULATION AND PROPER PRACTICES

All use of Mountview's networks must be in full compliance with English law and other regulations which are applicable.

Users must not try to gain unauthorised access to any system anywhere. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990.

Under The Terrorism Act 2000, The Counter Terrorism Act 2015 and as part of Mountview's safeguarding responsibilities, particularly responsibilities around the Prevent Duty, the Academy reserves the right to monitor computer and network usage to ensure users are acting safely and not open to or undertaking abuse or radicalisation.

Users must not do anything malicious, negligent or reckless which might cause any sort of harm or disruption to any computer system and associated programmes and data, or to any individual anywhere (worldwide). This includes any kind of damage, unauthorised access, denial of resources or any data alteration, and concerning individuals includes cyber-bullying, intimidation, harassment, grooming, blackmail and coercion.

Users must comply with valid regulations covering the use of any software or datasets, whether those regulations are made by law, by the producer or supplier of the software, by Mountview, or by any other legitimate authority.

The Data Protection Act 1998 regulates the use and storage of personal information on computing systems. It is each user's responsibility to ensure that their computer usage and information complies with this law. Failure to do so could result in criminal charges being brought against both you and the Academy.

3. CONDITIONS OF USE

3.1 USE OF MOUNTVIEW DEVICES

Any desktop, laptop, tablet or Mac computer equipment and all associated equipment such as keyboards, mice, monitors, USB sticks and other peripherals supplied by Mountview for users' use is the legal property of Mountview.

All users are given a username and password for appropriate access to their files and email accounts. Users must not try to use anyone else's username and password, and must not let anyone else use their username and password, which must remain confidential, except where this is required to be divulged and used in a formal investigation. Passwords should be changed regularly. For more information on passwords and best practice, see Appendix 1.

All users are responsible for the security of their Mountview computer equipment and for protecting any information or other data used and/or stored on them. Users must not allow their computer to be used by any unauthorised person. Computers being left unattended should be logged off or locked to prevent use by unauthorised persons, and minimum recommended computer settings should be set so that devices securely go into sleep mode if left idle to ensure device security.

The Mountview IT Service Desk reserves the right to install new software and updates to any Mountview computer device as and when necessary.

Mountview reserves the right to request the return of any Mountview IT equipment at any time, and all Mountview IT equipment must be returned to Mountview at the end of a user's employment or other working relationship with Mountview. Failure to return any equipment will result in action taken against the individual.

3.2 USE OF SOFTWARE ON MOUNTVIEW COMPUTERS

All software on any of Mountview's computers must be approved in advance by the Head of Facilities and Operations or IT Technician. Only authorised personnel may load software onto any of the Academy's computers, connect any hardware or other equipment to any such computers or move or change any such equipment.

Users must not make any copies of software except where this is expressly permitted by the copyright owner or as permitted by law. It is not permitted to use software for which Mountview does not own a current user licence. The taking of 'extra' copies of software or the introduction of software packages from sources outside the company is expressly prohibited.

If users have unlicensed software on a device for which they are responsible, they must advise the IT Service Desk so it can be removed immediately. This applies whether or not they actually use the software. If users are unsure whether they have a licence for a particular package, they should ask the IT Service Desk.

If a user needs a particular software package or are unsure as to whether they have appropriate licences for the software you are using, they must consult the Head of Facilities and Operations or IT Technician.

3.3 USE OF EMAIL

Mountview email accounts are for work or academic purposes and nothing should be sent from them that could compromise the Academy's reputation or security.

All users should be vigilant when handling attachments sent to them by email and not open anything from unfamiliar addresses. If users are in any doubt as to whether an attachment is genuine, contact the IT ServiceDesk.

All users should be vigilant to email 'phishing', the fraudulent practice of sending emails purporting to be from reputable companies or individuals (including purporting to be 'Mountview staff') to induce individuals to open attachments, click on links or reveal personal information such as passwords, credit card numbers or company data.

3.4 USE OF MOUNTVIEW DATA

All Mountview data must by default be considered to be confidential, and users must manage Mountview data in line with the relevant GDPR and Data Protection policies.

Unencrypted Mountview data must not be stored on any external device (such as USB stick or external hard drive). If users have a genuine need to use an external device for transferring data they must ensure the data is encrypted. Advice on this can be given by the IT Service Desk.

Loss of any device owned by Mountview or with access to Mountview data must be reported immediately to the Head of Facilities and Operations or IT Technician. Account passwords must be changed with immediate effect as soon as it becomes apparent that a device is missing.

3.5 USE OF PRIVATE AND PERSONAL EQUIPMENT

Privately owned equipment belonging to users must not connect to Mountview's wired or wireless staff network without authorisation from the IT Service Desk. Only privately owned equipment which is registered with the IT Technician, which (for Windows devices) has minimum Windows 11 specification, and which is virus free will be granted authorisation for network connection. Mountview reserves the right to install anti-virus and other software to allow remote security maintenance on these devices. Mountview accepts no responsibility for the effects that any such installation may have on the operability of privately owned devices, and consequently all risks reside with the owner.

Any devices, including but not limited to laptops, tablets and smartphones, must have a secure password lock to prevent unauthorised access if they are lost or stolen. This is particularly important for users with a Mountview account set up on their mobile device.

Users must inform the Head of Facilities & Operations or IT Technician immediately if a personal device is lost or stolen which has access to Mountview accounts or data.

3.6 USE OF MOUNTVIEW'S WIRELESS NETWORK

Users may use Mountview's wireless networks to gain access to the internet on private equipment including but not limited to laptops, tablets and smartphones.

When connected to Mountview's wired and wireless networks, Mountview equipment and privately owned equipment may be monitored in accordance with section 4 of this policy. Any equipment which is attributed to security problems or which causes security concerns may be disconnected without prior notification and in certain circumstances the user may be held accountable.

4. UNACCEPTABLE ACTIVITIES

Mountview's IT facilities must not generally be used for, or in connection with, the following unacceptable activities, some of which could result in legal action or civil proceedings being mounted against either an individual, the Academy, or both.

Mountview recognises that some of the following activities might overlap with official research or academic activity. Individuals must be able to justify any contravention conditions. Any user who wishes to carry out research activities contrary to the following unacceptable activities must notify the IT Service Desk of their intentions before using Mountview's equipment or networks for those purposes.

The unacceptable activities are:

I. Deliberately accessing, creating or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, with the exception of data which is connected with Mountview work or official research or other professional activity, where the sender/recipient would expect to exchange such material with other users in a professional capacity;
II. Creating, transmitting or accessing material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another, with the exception of data and email traffic which is connected with Academy work or official research or other professional activity, where the sender/recipient would expect to access or exchange such material with other users, in a professional capacity;

III. Creating, transmitting or accessing material which runs the risk of drawing people in to, or towards, terrorism.
IV. Deliberately contributing to news groups or websites that advocate illegal activity;
V. Creating or transmitting defamatory material or material that is libellous of any other individual or company's reputation, products or services;
VI. Viewing, transmitting, copying, downloading or producing material, including (but not limited to) software, films, television programmes, music, electronic documents and books which infringes the copyright of another individual or organisation;
VII. Making offensive or derogatory remarks about staff, students or Mountview on interactive social and lifestyle websites such as Facebook or Twitter;
VIII. Posting offensive, obscene or derogatory photographs, images, commentary or soundtracks on interactive social and lifestyle websites such as Facebook and YouTube
IX. Transmitting or producing material which breaches confidentiality undertakings;
X. Attempting to gain deliberate access to facilities or services which you are unauthorised to access;
XI. Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste user effort or networked resources;
XII. Creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe;
XIII. Making commitments via email or the Internet on behalf of the Academy without full authority;
XIV. Undertaking any activities detrimental to the reputation or business models of the Academy;
XV. Initiating or participating in the sending of chain letters, junk mail, spamming or other similar mailings.

Any user who inadvertently accesses an inappropriate Internet site must immediately close the session or return to the previous page.

Any user who receives an inappropriate email message or email content that appears to have been sent by another user, or who witnesses inappropriate use ofthe Internet by another user, must report the incident to their line manager or personal tutor. If the material seen reveals an immediate risk to another user, the user must follow the safeguarding procedures set out in Mountview's Safeguarding Policy.

5. PERSONAL USE OF MOUNTVIEW'S IT EQUIPMENT AND NETWORKS

5.1 PERSONAL USE OF INTERNET AND EMAIL

Significant bandwidth overheads are incurred through Internet and email traffic usage, and for email and attachment storage. In view of this, Mountview's IT equipment and networks are provided for operational and research purposes only. However, non-excessive and reasonable personal use of these facilities by users may be permitted provided that such use does not interfere with the work performance user, and is wholly compliant with legislative requirements and the terms of this policy.

Those who use Mountview's computing resources to make purchases, pay bills or conduct online banking or similar activities do so at their own risk. Mountview cannot be responsible for any direct or indirect losses sustained by those using its IT equipment or networks for personal transactions.

5.2 USE OF MOUNTVIEW EQUIPMENT AND NETWORKS FOR OUTSIDE WORK

Users must obtain permission from the Academy before using Mountview's computer equipment and/or networks for any work which is funded (partly or wholly) by any person or organisationoutside the Academy or on any consultancy basis. Permission for such work to be undertaken on Mountview equipment or networks may be refused, but where it is granted, a charge may be applicable.

6. MONITORING, PRIVACY AND THIRD PARTY ACCESS

6.1 MONITORING

Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) Mountview reserves the right to monitor users activities to:

I. Record evidence of official transactions;
II. Ensure compliance with regulatory or self-regulatory guidelines (including this policy);
III. Maintain effective operations or systems (e.g. preventing viruses);
IV. Prevent or detect criminal activity;
V. Prevent the unauthorised use of computer and telephone systems, i.e. ensure that the users do notbreach Mountview policies;
VI. Prevent the risk of harm, abuse, bullying, grooming and radicalisation to users as part of Mountview's safeguarding duty.

Under this regulation there is a requirement for employers to inform users about such monitoring. The publishing of this policy is one means of fulfilling that obligation.

In accordance with the above regulation, Mountview reserves the right to deploy software and systems that monitor, block or record all Internet access. These systems are capable of recording (for each and every user) exactly how much Internet usage is being conducted for each website visit (the date and time visited and how long was spent on the site), each email message and each file transfer into and out of Mountview's internal networks. This right is reserved at all times, although it is anticipated that instances of such monitoring will be minimal and proportional to operational needs.

Privately owned equipment connected to Mountview networks in accordance with 3.5 may be subjected to the same monitoring activities as Mountview equipment.

In certain investigatory circumstances it may be necessary for Mountview to access user emails, including emails which have been deleted. In such circumstances access will be proportionate tothe requirement for the access and subject to privacy assessment.

Access to users' emails will be undertaken under strict conditions and only on the authority of the Executive team. An audit trail will be maintained of all such access.

Logs of computer system usage will be taken and may be scrutinised. These will be retained for periods appropriate for operational purposes.

Data may be archived and Mountview reserves the right to examine this in accordance with 6.2 and to delete it.

6.2 PRIVACY AND THIRD PARTY ACCESS

A degree of privacy can be expected in the private use of Mountview's IT equipment and networks. However, all users should be aware that owing to the Academy's obligations (statutory and otherwise) there are limitations to the privacy that can be enjoyed.

For operational purposes it may be necessary for Mountview to access a user’s email folders and files

occasionally during periods of unexpected user absence, or in accordance with 6.1 above. This applies when no-one else (such as other departmental staff who are granted shared access to the user's account) can access the data required, and arrangements for them to do so could not have been made in advance of their absence.

Likewise, when users have ceased employment at Mountview it may be necessary for IT staff to recover or copy archived data that needs to be subsequently accessed by remaining and / or replacement staff.

With these points in mind, users should not use Mountview systems for the transmission or storage of personal material that they would not wish others to see.

Any Mountview user who is granted operational access to another user's data may only view material that is considered necessary to see for the operational reason for which access was granted. Theyare required to treat all material as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted, and they must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters. A failure to do so could constitute an offence under the terms of the Human Rights Act 2000.

It is stressed that any access to users' emails for data outside of the above controls could constitute a criminal offence.

7. SANCTIONS FOR BREACHES OF THIS POLICY

7.1 INTERNAL SANCTIONS

Where it is believed that a user of Mountview's IT equipment or networks has failed to comply with this policy, that user will face the Academy's Disciplinary Procedure. If the user is found to have breached this policy, they will face a disciplinary penalty ranging from verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the user's disciplinary record.

7.2 EXTERNAL SANCTIONS

Mountview expects users to use IT equipment and networks, in particular email and the Internet, responsibly at all times. Serious breach of this policy may result in referral to the police or to CHANNEL, a multi-agency network for targeting radicalisation, or other appropriate services.

8. RELATED POLICIES

IT Security Policy
Code of Practice for E-Safety and Online Communication
Data Protection Policy
Safeguarding Policy
Bullying and Harassment Policy
Student Disciplinary Procedure
Staff Disciplinary Procedure

APPENDIX 1: Passwords

It is the responsibility of each user to ensure that wherever possible any password used for Mountview IT equipment or networks should be as secure as possible. In addition it is vital that any passwords used for Mountview accounts or equipment are not identical to passwords used for personal accounts.

Please adhere to the following standards for passwords:

- Use complex passwords. That means a case-sensitive combination of letters, numbers, and special characters, at least ten in total.
- Do not reuse passwords or use the same password for more than one account. If one account hacked, attackers will use those known passwords to try and get into another service. Therefore it is imperative to use different passwords for each account you use.
- Change passwords regularly. Passwords should be changed at least once every 30 days.
- Mountview is increasingly operating an MFA policy for all accounts, including 3rd party software.

How to Choose a Better Password

Users should create passwords that are a balance between usability and security. Users should end up with a unique, complex password that should be simple to remember for the user, while providing significant protection against hacking.

Think of at least 3 or 4 random, unconnected words. Do not pick words that often appear together and definitely do not use phrases.

Give the password additional security by adding complexity; users must add capitals, numbers and symbols/punctuation. Try to add things into the middle of words, not just at the beginning or end.