Registered in England and Wales at
13 North Common Road, Ealing,
London, W5 2QB, Phone: 02088323071
Registered no: 2918520
Registered Charity no: 1050175

IT and Acceptable Use Policy

Metanoia Institute

Version Control

Document title: IT and Acceptable Use Policy	**No of pages: 12**
Version Number: 2.0	**Date first published: December 2021**
Approved by: Executive	**Last review date: June 2024**
Date originally approved: December 2021	**Due for next review: June 2027**

Related policies
• Disciplinary Policy • Anti-Harassment & Anti-Bullying Policy • Whistleblowing Policy • Grievance Policy • Equality, Diversity and Inclusion Policy • Data Protection Policy • Bring Your Own Device Acceptable Use Policy
External Reference

1. Contents

Metanoia Institute IT and Acceptable Use Policy

1. Policy Statement

This Policy explains how you as a person working in the capacity of staff member ("user") may use the Institute's computing facilities.

- how users or the Institute may be liable in law for misuse of the network facilities.
- how user's interests and the Institute's interests can be protected.
- the action which may be taken against users who fail to comply with the rules and regulations set out in this policy.

2. Scope

This Policy applies to all computer users within the Institute (including persons who are not staff or students but who have been authorised in writing by the Institute to use its network facilities), whether they use computers based at the Institute's premises or access the systems provided by the Institute via the internet using Institute-owned or private computing equipment. Compliance with this policy does not imply authorisation to use the Institute's computing facilities.

3. Important Considerations

- When using the Institute's computing facilities users must conduct themselves, at all times, in a lawful and appropriate manner so as not to discredit or harm the Institute or other users and at all times in accordance with the contents of this policy.

- The Institute's computing facilities are provided to assist with day-to-day work. Personal and recreational use is allowed; however, the Institute reserves the right to place whatever limitations it deems appropriate on such usage in order to safeguard the function of its computing facilities and users' compliance with any applicable laws and/or the contents of this policy.

- By using the Institute's network and computer systems, users provide their consent to having activity and accounts accessed, monitored, reviewed, recorded and stored without notice. The Institute may access the computer network system and review communications within the system in order to maintain it, investigate possible misuse, assure compliance with software copyright laws, comply with legal and regulatory requests for information, and other purpose deemed appropriate by the Institute.

- Users should not expect the use of the Institute's electronic communications to be private. Users will not be given notice when the Institute accesses electronic communications.

4. Basic Rules

- Only use the Institute's computing facilities for lawful activities. The Institute will not hesitate to contact the police if it discovers unlawful use of its computing facilities.

- Do not bypass the login procedure, this includes MFA.

- staff must ensure passwords are at least 12 characters to include upper case, lower case, numbers and special characters. Basic easy to guess passwords are not acceptable.
- If a password is suspected to be compromised staff or the Institutes, staff must alert the IT provider to immediately change it.

- Do not engage in any activity or omit doing anything which could jeopardise the integrity or security of the Institute's computing facilities.

- Keep your Network Identity, all your user accounts and associated passwords secure. Do not share your own or use someone else's network identity and user account.

- Managers may only access a user's account in their absence where the user has given their explicit approval. Approval should be sought from Human Resources where access to the user's account is required to ensure continuity of business services and where every reasonable effort has been made to seek the user's permission, but it has not been possible to contact the user.

- Do not use, or permit others to use, the Institute's computing network, equipment for any commercial use, nor for the purposes of endorsing or advertising such activity without the express authority of the Institute's Chief Executive Officer.

- Do not alter, interfere, add to or remove any physical part of the Institute's computing facilities or any equipment connected to or attached to the Institute's computing

facilities without authorisation.

- Do not access material, or attempt to access material, that you do not have permission to access.
- Do not deny (or do anything which denies) another users' legitimate access to the Institute's computing facilities.

- Do not connect any server, modem, wireless routers and hubs or network routers / switches / hubs to the Institute's computer network, or other similar transmitting device that operates on a wireless frequency without prior written agreement from the IT Department.
- Do not access company data/ platforms on public Wi-Fi systems.

- Do not make, store or transmit unlicensed copies of any trademark or copyrighted work (including software and media files).

- Do not send unsolicited bulk email messages, chain mail or spam.

- Do not deliberately or recklessly undertake activities which may result in any of the following the waste of other users' efforts or network resources, including time on any system accessible via the Institute network
- the corruption or disruption of other user's data
- the violation of the privacy of other users
- the disruption of the work of other users
- the introduction or transmission of a virus into the network

- To notify the Institute of any breach of security that may result in the compromise or loss of Institute data, files immediately.

- Before leaving the Institute, users must delete or arrange the transfer of all files and emails from their account. The Institute reserves all rights to access a leaver's emails and files for the purposes of ensuring the smooth continuity of business services.
- To return the Institutes loan equipment undamaged and in working order, normal usage wear and tear withstanding.

5. Internet use

- Do not, other than for ethically cleared, properly approved and lawful research purposes (as set out below) visit, view, store, download, transmit, display, print or distribute any material relating to:
    - sex or pornography.
    - lewd or obscene material of any nature or other material which may be likely to cause offence to another person.
    - terrorism or cults.
    - hate sites (racial or other).

- Users seeking authorisation for the above (for 'ethically cleared, properly approved and lawful research purposes') must obtain prior written approval from their Faculty Head or the appropriate member of the Executive and this approval needs to be reconfirmed in writing every 6 months. In addition, users should not intentionally do anything which enables others to visit, view, download, transmit, display, or distribute any material relating to the items listed above.

- Do not attempt to gain unauthorised access to any facility or service within or outside the Institute or make any attempt to disrupt or impair such a service.

- Do not setup or use hardware, or software, on the Institute's own internal network for the purpose of sniffing, hacking, network scanning or keyboard logging without prior written authorisation by the Institutes Chief Executive Officer.

- Do not alter or interfere with data, programs, files, electronic mail or other computer material which you do not have the right to alter.

- Do not post or present information in a way that may bring the Institute into disrepute or damage its reputation.

- Do not express opinions which purport to be the Institute's view unless you are authorised in writing to express views on behalf of the Institute.

6. Use of Online Platforms

- The Institutes online platforms are to be used in accordance with the following:

- Users must not alter or bypass security settings within accounts.

- The Institutes online platforms are provided and to be used solely for work and training purposes.

- Any recordings of online activities remain property of the Institute and shall not be distributed or displayed without prior consent from Executive.

7. Email use

- The Institute encourages its users to use email as a prompt and effective method of communication. Email services are provided to users primarily for bona-fide business purposes, although limited personal use is allowed. The Institute reserves the right to place whatever limitations it deems appropriate on such usage to safeguard the primary function of its own network.

- Users must act responsibly and appropriately when using the Institute's computing facilities to send email, whether internally or externally using the Internet.

- No user should send any email that contains any material that the Institute considers or might reasonably be considered by the recipient to be bullying, harassing, obscene, racist, sexist, defamatory, offensive, "chain mail", incitement to commit a criminal offence or threatening or which contains any malicious code; for example, a virus. If you receive an email containing any such material, and you are concerned about this you should inform your line manager.

- Users must not send email which might bring the Institute into disrepute or purport to be the view(s) of the Institute unless the user is authorised in writing to express views on behalf of the Institute.
- The creation and usage of distribution lists/groups should be monitored by the owner, distribution lists should only hold relevant staff to the group within the Institute, and owners are required to maintain membership.
- All staff must check when using distribution lists/groups that only relevant staff are included in membership before emailing a specific distribution list/group.

- The Institute reserves the right to automatically delete email which contains viruses.

- Users hereby agree that emails generated by, or stored on, the Institute's computers are the Institute's property; and may be subject to review and disclosure under the Freedom of Information Act and General Data Protection Regulation as well as potentially disclosable and admissible in evidence, in a dispute.

8. Telephone System Use

- Use of the Institute's telephone system, including Institute owned mobile equipment, is primarily for business purposes only.

- Users must act responsibly and appropriately when taking calls in shared offices and/or spaces. Caution must always be exercised to safeguard the confidentiality of the Institute's personal data.

- Reasonable limited personal use is permitted for local calls, provided this does not interfere with your work or business use. If you are found to be abusing this facility you may be subject to disciplinary action.

- Long-distance or international personal calls are not permitted.

- Users must act responsibly and appropriately when taking personal calls on their

mobile devices in shared offices and/or spaces. Caution must always be exercised to safeguard the confidentiality of the Institute's personal data.

- Any breach of these rules may be considered as misconduct and may result in disciplinary action being taken, including dismissal.

9. Legitimate Use

There may be circumstances where a user feels that the nature of their work or studies means they have a legitimate reason for accessing and/or using material prohibited under this policy. In this circumstance the user must discuss this with their Line Manager/Faculty Head in advance as to the precise reasons for such access and use and no such access and/or use may be undertaken without their express written approval.

10. Unacceptable Conduct

- Emails and the internet are considered to be a form of publication and therefore the use of the Internet, email and the making available of any information online, must not be offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material. Misuse of email or inappropriate use of the Internet by viewing, accessing, transmitting or downloading any such offensive information will amount to gross misconduct in accordance with the terms of the user's contract of employment and may result in summary dismissal and/or withdrawal of services.

- Words and pictures produced on the Internet can be defamatory if, for instance, they are untrue, ridicule a person and damage that person's reputation. For these purposes, as well as any individuals, a "person" may include the Institute or another institution. You must not create or transmit any offensive or defamatory statement while using the Internet or the Institute's computing facilities, whether in emails or otherwise. As well as your being personally exposed to potential legal action for defamation, the Institute would also be held liable.

- It is a criminal offence to publish or distribute obscene material or to display indecent material in public. The Internet or any computer 'message boards' qualify as a public place. The accessing or sending of obscene or indecent material using the Institute's computing facilities is strictly forbidden and in accordance with the terms of the user's contract of employment and may result in summary dismissal and/or withdrawal of services.

11. Discrimination and Harassment

The Institute does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on the Institute's computing facilities or via the Internet. Users should not view, use or distribute any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability.

12. Security

- It is each user's responsibility to log off from or lock the system when leaving the computer unattended to avoid inadvertent security breaches.

- Users must not disclose (including by sending via or placing on the Internet) any material which incites or encourages or enables others to gain unauthorised access to the Institute's computer facilities.

- It is vital that all users take all necessary steps to safeguard the Institute's computer facilities from viruses e.g. reporting suspicious unsolicited emails or attachments.

13. Data Protection

- Any work involving processing, storing or recording personal data (information on an identifiable living individual) is governed by the General Data Protection Regulation 2018. It is the user's responsibility to ensure that personal data is collected and used in accordance with the legislation. Further information can be obtained from the Institute's Data Protection Policy.

- If you believe that your work involves the processing, storing or recording of personal data, you must first seek confirmation from the Data Protection Officer that consent

has been obtained. The Data Protection Officer can be contacted via dataprotection@metanoia.ac.uk.

14. Third-Party Data Storage / Cloud Services

Please refer to the Institute's Bring Your Own Device Acceptable Use Policy for information.

For any further questions and advice before proceeding, staff are advised to contact the IT Department and the Data Protection Officer.

15. Monitoring

- The Institute reserves the right without notice to monitor users' usage of the Institute's computing facilities and to access data held on the Institute's computing facilities for justifiable business purposes and in order to perform various legal obligations including:

    - where it is suspected that a User is misusing the Institute's computing facilities.
    - to investigate misuse of the Institute's computing facilities.
    - where the Institute has received a request from an authorised external party to monitor a User's use of the Institute's computing facilities.
    - to prevent or detect crime (including 'hacking');
    - to resolve system performance problems which may otherwise damage the computing services provided to other Institute users; or
    - to intercept emails for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations.

- The Institute reserves the right to automatically block certain network protocols and sites in order to minimize the risk of viruses, hacking, network scanning and other inappropriate file transfer activities.

- The Institute maintains logs of user and network activity which may be used in investigations of breaches of Institute computing regulations, performance monitoring or provision of statistical reports.

The Institute reserves the right to make and keep copies of emails and data documenting use of email and/or the Internet systems, for the purposes set out above. Users hereby acknowledge and agree that the Institute has the right to retain or delete copies of any data stored on the system in order to comply with its statutory obligations or, at its own discretion, in accordance with the legitimate purposes stated above.

In using the Institute's computing facilities, users implicitly accept this policy. Consequently, users agree to their activities being monitored in the circumstances given above.

16. Liability for Misuse and Disciplinary Action

Users and the Institute are potentially at risk for a range of civil and criminal liability arising from misuse of the Institute's computing facilities. Legal liability can arise from:

- defamation under the Defamation Acts.
- copyright infringement under the Copyright, Designs and Patent Act.
- breach of confidence.
- negligent virus transmission.
- computer hacking and any breach of the Computer Misuse Act and the Police and Justice Act.
- Breach of the Obscene Publications Acts, the Protection of Children Act and the Telecommunications Act;
- harassment and discrimination under the Equality Act.
- the General Data Protection Regulation and the Human Rights Act.
- the Regulation of Investigatory Powers Act, the Terrorism Act and the Serious Organized Crime and Police Act.

Misuse of the Institute's computing facilities (including failing to comply with this policy) may expose both users personally and/or the Institute to court proceedings attracting both criminal and civil liability. Users will be held responsible for any claims brought against the Institute for any legal action to which the Institute is, or might be, exposed as a result of user's misuse of the Institute's computing facilities including reimbursing the Institute for any financial liability which the Institute suffers as a result of users' actions or omissions.

- The Institute considers failure or refusal to comply with this policy to be a disciplinary offence which may lead to disciplinary action taken, including dismissal without notice and/or withdrawal of services. Action will be taken in accordance with the user's contract of employment (or work order) with the Institute.

17. Firewall Policy

- Only our IT provider has external access to manage our firewalls, this access is restricted to their management IP address.
- TCP Port 443 is open an North Common Road staff firewall, to allow access to Remote Desktop via Remote Desktop Web Access and Gateway Server which uses TCP Port 443 to provide access via RDP over HTTPs.
- External passwords must be a minimum of 12 characters.

18. Monitoring and Review

Human Resources are responsible for monitoring the effectiveness of this policy and supporting procedures and will conduct reviews at appropriate intervals. Anyone who feels they have been unfairly treated or discriminated against should contact Human Resources.