13 – Appendix 1

MERSEYSIDE RECYCLING & WASTE AUTHORITY

2025

Acceptable Use Policy

ICT-POL-001

MICHAEL NICHOLLS

Acceptable Use Policy

1 Document Control

Field	Details
Document Title	Acceptable Use Policy
Document ID	ICT-POL-001
Version	1.0
Author	Michael Nicholls
Approver	Paula Pocock
Date of Issue	30/12/2025
Next Review Date	
Status	Draft

2 Revision History

Version	Date	Author	Description
1.0	30/12/2025	Michael Nicholls	Initial Draft

3 Distribution

Name	Role

4 Approval

Name	Role	Signature	Date

5 Contents

Table of Contents

6 Purpose

The purpose of the Acceptable Use Policy (AUP) is to set out the acceptable and secure use of all the Authority's ICT resources, data and digital services to:

- Protect residents, staff, and the Authority's reputation.
- Comply with legal and regulatory requirements (e.g., UK GDPR, Data Protection Act 2018).
- Reduce cyber risk and enable efficient service delivery.
- Provide clear expectations and responsibilities for all users of MRWA systems

7 Scope

This AUP applies to all:

- Staff: Employees, contractors, consultants, and third-party users.
- Devices: Authority-issued laptops, desktops, mobiles and tablets,
- Systems & Services: Network, email, internet, telephony/Voice over IP, cloud platforms
- Data: All Authority data (public, internal, confidential, special category/personal data), and third-party data held by the Authority.

8 Roles & Responsibilities

- All Users: Follow this AUP; protect accounts and data; report incidents (including loss, theft, damage or unauthorised use) immediately to line managers, follow Health and Safety advice as issued for electrical safety checks and VDU assessments.
- Managers: Ensure staff awareness, induction, and compliance; escalate violations.
- ICT Team: Provide secure services, monitoring, access controls, incident response, patching.
- System owners: Define appropriate use for their systems; manage permissions.

9 Definitions

- ICT Resources: Includes hardware, software, network services, electronic messaging, internet access, and cloud services provided by the authority.
- Personal Data: Any information relating to an identified or identifiable individual, as defined under GDPR.
- Sensitive Data: Data classified as confidential or restricted under the authority's Data Classification Policy.

10 Policy Principles

10.1 Acceptable Use

- ICT Resources must be used primarily for authorised official use.
- Transparency & Accountability: Communicate openly and accurately.
- Political Neutrality: Maintain impartiality, especially during pre-election periods.
- Only access ICT Resources as required for their role.
- Access only data and systems you are authorised to use.
- Store and share Authority data in approved locations

10.2 Unacceptable Use

- View, create, store, or transmit illegal, discriminatory, abusive, or sexually explicit content.
- Harm the Authority's reputation or systems.
- Infringe copyright or licence terms; use pirated materials.
- Conduct private business or political campaigning using ICT resources.

11 Security Compliance

11.1 Acceptable Use

- Use strong, unique passwords and multi-factor authentication.
- Install updates as prompted.
- Mobile devices should be stored securely out of view in a locked vehicle or home. They should not be left unattended in public places.
- Lock devices when unattended.
- Avoid public Wi-Fi for sensitive work.
- Encrypt sensitive data when transmitting externally.
- Report phishing attempts, suspicious websites, or security incidents immediately to ICT.

11.2 Unacceptable Use

- Install unauthorised software.
- Email Sensitive data without approved safeguards.
- Share passwords, MFA codes, or authentication tokens of own accounts
- Connect unapproved devices to the corporate network.
- Attempt to bypass security controls.
- Leave devices unlocked or unattended.
- Auto-forward Authority email to personal accounts.
- Copy Authority data to personal devices, or unapproved storage.

12 Internet

12.1 Acceptable Use

Use of the Internet is available at your line manager’s discretion.

In general, users shall only use the Internet for official purposes. Use of information from the Internet should be directly related to the official duties of the user, or the Authority as a whole. All information downloaded from the Internet shall be related to the duties and tasks of the user. However, reasonable personal use is permitted in the users own time if it does not interfere with tasks of the user.

Users must check the quality and accuracy of information from the internet before using it for Authority purposes and use independent sources to verify if necessary.

No personally owned ICT equipment may be attached to the Authority’s network.

12.2 Personal Use

Any reasonable personal use of the Authority’s ICT services and equipment must comply with the Authority’s Codes of Conduct for Officers.

Reasonable personal use of such services and equipment:

- Should not interfere with the performance of your duties.
- Should not take priority over your work responsibilities.
- Should not result in the Authority incurring expense.
- Should not have a negative impact on the Authority.
- Should be lawful and in accordance with the Authority Policy and the Guidelines as set out in this document.

Where reasonable personal use is referred to in this document, this section applies.

12.3 Unacceptable Use

The internet connection from any Authority owned or managed device must not be used for any illegal or unethical activity, or personal business activity, and must not be used to compromise the security of any computer system or network.

There must be no personal financial activity: (e.g. shopping, entering competitions, gambling, use of credit cards, financial services etc.) The Authority will not be held responsible for any fraudulent actions.

Users must not intentionally access or transmit information which is obscene, sexually explicit, racist or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to Authority policy.

The downloading of entertainment software, games, music or the playing of games against an opponent via the Internet is forbidden.

Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

Users must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

Accessing the internet from another employee’s device is not permitted unless the user is logged on with their own username and password.

Other examples of Computer Misuse can include the following:

- computer hacking (accessing another computer without permission)
- providing access to unauthorised persons (including minors)
- impersonation
- gaming, wagering or betting
- the intentional transmission in any way of malware or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files)
- downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications)
- disclosing private or confidential information, including passwords or other information, that may compromise the security of systems and networks
- Accessing, creating, or distributing illegal, offensive, discriminatory, or extremist material.
- Political campaigning or unauthorised commercial activities.
- Circumventing security controls or installing unapproved software.

13 Social Media

13.1 Acceptable Use

You must be authorised to use the social media account and to represent MRWA to the public as part of your job role. Only authorised accounts should be used to publish messages and respond to other users of the social media channel. Do not use your own personal account.

When posting or engaging with other users, always make it clear that you work for MRWA and are representing us as an organisation. Never pretend to be someone you are not. Be careful what information you share online about customers, other employees, financial information, business operations or anything else that might be private or confidential. Give due regard to the Copyright Designs and Patent Act 1988.

13.2 Personal Use

This policy relates to the business use of social media but also covers some areas of personal use of social media. If employees (that have been granted access to corporate social media) are found to be accessing social media sites for personal reasons, then appropriate action will be taken. Employees who access social media sites during their own time (e.g. during lunch break or outside of work time) must also be aware that inappropriate activity linking them to the Authority will be investigated and action may be taken.

Employees should be aware that the Code of Conduct for Officers covers the use of fidelity and information disclosure and should bear this in mind when using social media (in a personal capacity) outside work. Employees should be aware that any reports of inappropriate activity linking them to the Authority, will be investigated and action may be taken.

13.3 Unacceptable Use

- Sharing confidential data or internal documents.
- Posting discriminatory, harassing, or defamatory content.
- Using Authority accounts for personal or political purposes.

14 Email, Messaging & Collaboration

14.1 Acceptable Use

The Authority provided electronic messaging facilities must always be used when communicating with others on official business. You must not use a personal account for this purpose. All communication must be professional and respectful. Limited personal use is permitted if it does not interfere with duties and the message is labelled as personal.

Users must always use their own unique email address when sending emails, even when answering emails sent to another user unless it is a generic account that you have been authorised to send on behalf of.

All messages sent from an Authority account remain the property of MRWA and are part of the corporate record. All Authority messages should be considered as official communications from the Authority and treated accordingly.

Users should take care when replying to messages and only reply to all recipients when it is necessary that every recipient should receive the message. Care must be taken when addressing messages that include confidential information to prevent accidental transmission to unauthorised recipients. Users should also pay attention to how a message can be interpreted when read by the recipient taking into consideration their culture and their role.

When using electronic messaging facilities as a means of communication, it should be kept in mind that:

- Electronic messages are potentially subject to disclosure under the Freedom of Information Act 2000, including all expressions of fact, intent, and opinion.
- Electronic messages may also be produced in court in the same manner as any other document.
- Advice given by e-mail has the same legal effect as that given in any written format.
- Electronic messages, either internally or externally, are neither guaranteed to be private nor to arrive at their destination either on time or at all.
- Advice given by email has the same legal effect as that given in any written format.
- All emails will have the Authority's agreed disclaimer within the signature.
- Consider use of SharePoint for sharing large/sensitive documents as an alternative to sending an attachment. This offers advanced document control methods such as restricted download or viewing only options.

14.2 Unacceptable Use

Users must not forward material which has been emailed to them directly without the permission of the originator unless the information is forwarded for reasons of normal Authority business.

Users must not falsify electronic messages to appear as if sent from someone else or to provide false information to any Internet service requiring an email address or other details.

Users should not open electronic attachments if the source of such an attachment is unclear. Any suspicious attachments should be reported but not sent to the ICT Team for further investigation.

Users must not take part in discussions on political matters via either the Internet or e-mail unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

Users must not read, delete, copy, or modify the contents of the mailbox of another employee or member without the proper authority, which is generally the authorisation of the line manager of the employee whose mailbox is being accessed.

Official Authority electronic messaging facilities must not be used:

- For the distribution of unsolicited commercial or advertising material or other junk-mail of any kind, to other organisations
- To send material that infringes the copyright or intellectual property rights of another person or organisation.
- To distribute any offensive, obscene or indecent images,

- To send anything which is designed or likely to cause annoyance, inconvenience, or needless anxiety to others.
- To convey abusive, threatening or bullying messages to others
- To transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs.
- Transmission of defamatory material or false claims of a deceptive nature
- For activities that violate the privacy of other users
- To send anonymous messages - i.e. without clear identification of the sender
- For any other activities which bring, or may bring, the Authority into disrepute.

14.3 Encryption Requirements

- All emails containing personal, sensitive, or confidential data must use Authority approved encryption tools.
- Sensitive files must be encrypted before sending.
- Passwords for encrypted files must be shared via a separate secure channel.
- Only use platforms with end-to-end encryption (e.g., Microsoft Teams, WhatsApp).
- Do not send unencrypted sensitive data via SMS or non-approved apps.

14.4 Group Chats

Group chats must:

- Be created only for legitimate Authority business.
- Have a designated owner or administrator responsible for compliance.
- Include only relevant participants.

Sensitive discussions should not occur in group chats unless the platform is approved for secure communication. Decisions made in group chats must be documented in official systems. Group chats are subject to FOI and retention requirements. This applies to any device that the group chat takes place on.

15 AI

15.1 Acceptable Use

Copilot will be the Authority’s AI tool, and no other AI tool will be permitted unless specifically authorised.

Copilot can be used for the following purposes:

- Drafting reports, emails, and documentation.
- Summarising non-sensitive information.
- Improving clarity of written reports / emails / briefings

- Converting notes into structured formats (agenda, bullets, actions).
- Generating ideas and improving productivity.

15.2 Unacceptable Use

- Inputting sensitive or personal data unless explicitly approved
- Autonomous decision-making impacting individuals or services
- Create, distribute, or promote any content that is unlawful, offensive, obscene, defamatory, hateful, discriminatory, or otherwise objectionable.
- Generate or transmit any malicious code, such as viruses, worms, trojans, ransomware, etc.

15.3 Data Handling

It is essential that no Personally Identifiable Information or confidential data is inputted into AI at any time. Information outputted from Copilot needs to be validated for accuracy, bias, and compliance before use. It has been known that AI can often produce inaccurate information, and this must always be checked and verified before being circulated.

16 Data Protection

- Users must make sure to handle personal and sensitive data in accordance with GDPR and the Authority's Data Protection Policy.
- Do not share confidential information without proper authorisation.
- Store data only on approved systems and locations.
- Users should be aware of displaying sensitive information visible on the screen when using in a public area.
- All devices should be stored securely and out of view when not been used.

17 Monitoring and Compliance

The Authority reserves the right to monitor all activity on all Authority owned ICT Resources for security and compliance purposes in line with GDPR.

In the case of an investigation, the Business Services Manager will access the necessary monitored information and provide a report of this to the relevant Manager.

18 Consequences of Non-Compliance

Breach of this policy may result in:

- Disciplinary action (see disciplinary policy)
- Legal action where applicable.

19 Related Policies

This UAP should be read alongside:

- the Code of Conduct
- the Publication Scheme,
- the Communications Strategy
- the Disciplinary Procedure

20 Acknowledgement Form

All users must confirm they have read, understood, and agree to comply with this policy before accessing the Authority's ICT Resources.