W·R·W·A

Acceptable Use of Equipment and Data Policy

12th June 2025

Introduction

This Acceptable Use Policy aims to ensure that staff members understand their responsibilities for the appropriate use of WRWA's information technology resources. Understanding what is expected will help staff members to protect themselves, colleagues and WRWA's equipment, information and reputation and ensure that there is clear accountability.

Scope

All WRWA equipment and information (all information systems, hardware, software, and channels of communication, including telephone, social media, video, email, instant messaging, internet). User's personal information which is processed by WRWA equipment is also subject to this policy.

Who this policy applies to?

All WRWA staff members with access to WRWA's information and information systems and assets.

1. Acceptable Use Principles

1. General Principles

Staff members must:

1.1 Confirm that they agree to complying with this policy and understand that breaching this policy may result in disciplinary procedures.

1.2 Be responsible for their own actions and act responsibly and professionally, at all times.

1.3 Immediately report any breach of this Acceptable Use Policy to their line manager.

1.4 Never undertake illegal activity, or any activity that would be harmful to WRWA's reputation or jeopardise staff and/or resident's data, on WRWA technology.

1.5 Understand that WRWA reserve the right to monitor the use of officer equipment, internet usage and communication.

1.6 Understand that they can use the WRWA Whistleblowing Code, and raise a concern, if it is believed that someone is misusing WRWA assets, information, or electronic equipment.

1.7 Undertake education and awareness training on security when using WRWA information and technology, when contacted to do so by the WRWA Finance and Administration Officer, in order to support their understanding of recognising and reporting threats, risks, vulnerabilities and incidents.

2. User IDs and Passwords

Staff members must:

2.1 Protect usernames and passwords appropriately.

2.2 Create secure passwords following relevant WRWA instructions. Passwords must not be stored in shared folders or written down.

2.3 Not log on to any WRWA systems using a colleague's credentials.

2.4 Log out of all computer devices connected to WRWA's internal network during non-working hours, i.e., at the end of the working day.

3. Managing and Protecting Information

Staff members must:

3.1 Understand that they and WRWA have a legal responsibility to protect personal and sensitive information and must not misuse their official position to further private interests, or those of others.

3.2 Ensure that all information is created, used, shared, and disposed of in line with business need.

3.3 Not attempt to access anyone's personal data unless there is a legitimate business need that is appropriate to their job role.

4. Personal Use of WRWA IT

Staff members must:

4.1 Understand that they are personally accountable for what they do online and with WRWA technology.

4.2 Understand that WRWA does not allow personal use of its IT resources in contracted hours or in an employee's own time when not on official duty.

4.3 Not access personal webmail accounts on WRWA equipment.

4.4 Follow the WRWA Employee Code of Conduct and must not:

- Trade or canvass support for any organisation on official premises, whether it is for personal gain from any type of transaction or on behalf of external bodies,
- Provide unauthorised views or commitments that could appear to be on behalf of WRWA,
- Use behaviour that is discriminatory in any sense (e.g., on the grounds of sex, sexual orientation, gender, race, age, religious beliefs, or disability),
- Download software onto WRWA devices with the exception of those permitted by WRWA which will always be from an official source and appropriately licensed. This software must not compromise the performance or security of the device,
- Download music, video or other media-related files for non-business purposes or store such files on network drives.

5. Email/Communication Tools

Staff members must:

5.1 Only use professional Communication and appropriate language in messages, emails and recordings.

5.2 Not disclose sensitive and confidential information through emails or any other communication tools.

5.3 Not alter the content of a third party's message when forwarding it unless authorised to do so i.e. it is necessary to redact personal information.

5.4 Be vigilant to scam targeting communications especially phishing emails and know how to spot and report suspicious emails.

5.5 Not use their WRWA email address for personal use. Only use your WRWA email address for WRWA business related activities and linked organisational activity (e.g. Trade Union activity and other officially provided Internet links).

6. Websites and Social Media

Staff members must:

6.1 Use social media appropriately and understand that the principles covering the use of social media by WRWA staff in either their official or personal capacity are the same as those that apply for any other activity and that they are responsible for the content they post.

6.2 Only use approved WRWA social media accounts for official business and where appropriate, use WRWA branding and a professional image or persona on such accounts.

6.3 Understand that their social media content/footprint may be available for anyone to see, indexed by Google and archived for posterity.

6.4 Only access appropriate content using WRWA technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity.

7. Devices, Systems and Networks

7.1 Only use systems, applications, software, and devices (including USBs, laptops, and smart phones), which are approved, procured and configuration managed by WRWA when undertaking official business, and apply WRWA standards and guidance in their use.

7.2 Staff members with WRWA mobile phones must always install the most up to date software when it becomes available as this ensures the device has the latest security updates installed.

7.3 When staff members are required to generate a two-factor authentication onetime password to access a WRWA system, use of a personal device is permitted in the absence of a WRWA device.

7.4 The use of personal Bluetooth headsets, keyboards and mice are permitted when paired with WRWA devices that are enabled to support the connectivity. Bluetooth connection must be compatible with WRWA devices and staff members must not download any software onto WRWA devices to conduct the pairing of Bluetooth.

7.5 WRWA permits the use of personal mobile phones and personal landline numbers for voice calls in exceptional circumstances only, which include internal calls to colleagues within WRWA, other Government Departments, Local Authorities, and the supply chain/business partners however personal or sensitive information should not be discussed. Where a staff member has access to a WRWA phone or a Softphone (Avaya) on their WRWA device, these must be used as they are the WRWA's preferred method of communication. Employees must not use personal phones to contact residents or their appointed agents as this still remains prohibited.

7.6 WRWA permits connecting WRWA devices, laptops etc., by Wi-Fi (or Ethernet) to the internet from anywhere e.g., home or a hotel. However, WRWA devices must not be connected to the internet via Captive Portals, for security reasons. WRWA devices are set up so they do not connect to Captive Portals.

7.7 WRWA permits wirelessly connecting a WRWA device to a WRWA, or personal, mobile phone via a personal hotspot for the purpose of acquiring an internet connection (tethering) for work purposes. Tethering a personal mobile phone is permissible but WRWA cannot be held liable for this use of a personal mobile phone including any data charges, and so any use of a personal phone for this purpose is the individual's choice.

7.8 Do not use any personal wallpapers or screensavers. The use of personal background settings (e.g., MS Teams), images (e.g., Outlook profile) etc. is permitted on WRWA devices but must be respectful and must not contain any inappropriate or offensive material that may bring the individual or WRWA into professional disrepute.

7.9 Staff members should raise all software requests through the Finance and Administration Officer.

8. Physical Security

Staff members must:

8.1 Be responsible for keeping all portable devices assigned to them safe and secure and immediately report any loss or damage of their equipment to the Finance and Administration Officer.

8.2 Bring the equipment to the office for PAT testing when requested to do so.

8.3 Protect WRWA equipment appropriately when travelling e.g.

- Laptops must always be carried as hand luggage
- Never leave a portable device visible in parked vehicles

- Never leave equipment unattended in a public place e.g., on public transport.

8.4 Return all WRWA assets when leaving WRWA. Failure to return equipment could lead to steps being taken to recover the cost, which could include legal action through the civil courts.

8.5 The Finance and Administration Officer must complete all appropriate exit procedures with leavers.

9. Compliance

9.1 If for any reason staff members are unable to comply with this policy, or require use of technology which is outside its scope, this should be discussed with their line manager in the first instance.

9.2 Line managers are responsible for ensuring that staff members understand their responsibilities and consequences as defined in this policy and continue to meet its requirements for the duration of their employment with WRWA. This does not remove responsibility from staff members, who must ensure that they too understand their responsibilities as outlined in this policy and continue to meet the requirements. It is a line manager's responsibility to take appropriate action if staff members fail to comply with this policy.

9.3 WRWA will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems, design and processes and speak to people to facilitate this. All WRWA staff members will be required to facilitate, support, and when necessary, participate in any such inspection.

9.4 Failure to report a security incident, potential or otherwise, could result in disciplinary action.

9.5 Breaching this policy may result in disciplinary prosecution.