INFORMATION COMMUNICATION TECHNOLOGY POLICIES REVIEW
WDA/07/26

Recommendation

That Members:

1) Approve the Draft Acceptable Use Policy at Appendix 1 of this report.

2) Note the findings from a review of the Authority's Information Communications Technology policies.

THIS PAGE INTENTIONALLY BLANK

INFORMATION COMMUNICATION TECHNOLOGY POLICIES REVIEW
WDA/07/26

Report of the Chief Executive

1. Purpose of the Report

1.1 This report provides an update on the review of the Authority's Information Communication Technology (ICT) policies and asks Members to approve a new Acceptable Use Policy (AUP) which encompasses the principles of the existing Social Media and Internet Policy, and Email Policy.

2. Background

2.1 Cyber Essentials Plus is a recognised accreditation demonstrating that ICT systems are well governed, compliant with the latest requirements for cyber security, and that they are monitored and maintained. An organisation's Policies, Procedures and staff awareness forms a large part of the assessment. MWDA aspire to accreditation in 2026.

2.2 An AUP is an essential document for accreditation and ensuring users of the Authority's systems understand their responsibilities and the best practices that should be adhered to.

2.3 A new Information Communication Technology (ICT) System was implemented in 2024. A Customer Relationship Management System was developed to replace legacy applications in 2025.

2.4 Existing Authority policies governing ICT resource usage required a review to ensure documentation accurately reflected the changes in MWDA's ICT technology, current best practice guidance and the capabilities now available to MWDA employees. Current, relevant, Policies and awareness are vital preparation for accreditation.

3. ICT Policy Review

3.1 The Authority had previously operated under the Liverpool City Region Combined Authority User Policy as they had previously provisioned MWDA's ICT. The review identified the need to develop an Authority specific AUP relating to current ICT provision, equipment, capabilities and new systems.

3.2 It was established that the principles set out in the existing Email and Internet Policy remained fundamentally accurate but the policy did not encompass the wider range of options available for electronic messaging utilised today or reflect the best practice options for sharing sensitive information or large attachments. Artificial Intelligence needed to be included as this is a growing technology that is increasingly available and MWDA recognises both the opportunities and risks it presents.

3.3 The social media policy was reviewed and the principles and guidance in the document remained valid.

4. Acceptable Use Policy

4.1 The Draft AUP at appendix 1, provides clear expectations and responsibilities for all users of MWDA systems and encompasses the principles from the existing Email and Internet Policy and Social Media Policy. If approved by Members, it will replace these policies.

4.2 Combining the policies reduces repetition of acceptable and non acceptable use across all ICT related documents whilst providing a single point of information and reference for all employees.

4.3 Adherence to the draft AUP, will protect data, staff, and the Authority's reputation, ensure compliance with legal and regulatory requirements, reduce cyber risk and enable efficient ICT service delivery. It is also a vital step towards readiness for accreditation.

4.4 Members are asked to approve the draft AUP attached at Appendix 1.

5. Risk Implications

Identified Risk	Likelihood Rating	Consequence Rating	Risk Value	Mitigation
Unclear policy on acceptable use could result in inappropriate use of ICT resources and reputational damage	2	5	10	Introduce a high level, all encompassing AUP covering all ICT resources and usage.
Failure to comply with recognised Cyber Security Frameworks	3	5	15	An agreed AUP will assist with accreditation

would prevent accreditation, potentially affecting insurance cover and limit opportunities for partnership working in the future.				

6. HR Implications

6.1 Employees will be informed that compliance and monitoring will take place and that breach of policy could result in Disciplinary action.

6.2 At the point of acceptance, employees will be reminded the Authority is legally obliged to co-operate with the Police, and HM Revenues and Customs, in the investigation and detection of crime and apprehension of offenders. And that this may involve allowing such bodies' access to the monitoring records of or equipment held by an individual employee.

7. Environmental Implications

7.1 None directly associated with this report.

8. Financial Implications

8.1 None directly associated with this report.

9. Legal Implications

9.1 Employees should note that all electronic messaging on Authority equipment is subject to disclosure in a court of law and FOIA requests. GDPR compliance and Document Retention periods are also applicable.

10. Conclusion

10.1 The review highlighted the Authority lacked a MWDA specific Acceptable Use Policy. It was considered the principles of the Email and Internet Policy and Social Media policy remained valid but the former did not reflect current ICT options and capabilities hence updates were required. The opportunity arose to combine ICT policies into a single source of information. The resulting draft AUP clearly states the Authority's position regards use of its ICT systems and promotes industry best practice.

10.2 The draft Acceptable Use Policy, if approved, will increase security, reduce risk of cyber attack, ensure ICT service delivery and contribute to readiness for Cyber Essentials Plus Accreditation.

10.3 It is recommended that Members:

- Approve the draft Acceptable Use Policy at Appendix 1 of this report.

The contact officer for this report is: Nicola Hodge
7th Floor, Number 1 Mann Island, Liverpool, L3 1BP

Email: Nicola.Hodge@merseysidewda.gov.uk
Tel: 0151 255 2547
The background documents to this report are open to inspection in accordance with Section 100D of The Local Government Act 1972 - Nil.