Policy A5 – Information Services

1. Policy Intention

This policy outlines the conditions governing the use of all Information Services facilities provided by the Shire of Murray (Shire). The policy applies to Council Members, staff and to others to whom access to Information Services will be provided.

2. Policy

2.1 General Use

2.1.1 The Shire reserves the right to, without notice, modify, upgrade, withdraw or otherwise alter any facilities provided.

2.1.2 The Shire has ownership of all files and e-mail messages stored on Shire computers and reserves the right to examine all computer data and software on its facilities and to monitor usage in order to ensure compliance with this Policy.

2.1.3 Any facilities provided to users are for the business purposes of the Shire. The Shire will not be responsible for meeting any costs resulting from either the misuse of facilities or the use of facilities for non-business-related purposes.

2.1.4 The Shire supports only those facilities which it provides for business purposes. Hardware, software, operating systems and networking protocols not in use at, or provided and approved by the Shire Information Services Department, are not supported.

2.2 Storage

2.2.1 All corporate information including correspondence, minutes of meetings, memos, file notes and reports (other than those generated through the Shire's databases) are to be stored in the Electronic Document Management System (EDMS). This is consistent with the legislative requirements of the *State Records Act 2000*.

2.2.2 E-mails and faxes, sent and received, and of corporate nature must be captured and stored in the EDMS. This is consistent with the legislative requirements of the *State Records Act 2000.*

2.2.3 Hard copy documents must be scanned and registered into the EDMS immediately upon receipt.

2.2.4 Corporate documents must not be stored on desktop computers, or on portable media or uploaded to personal cloud storage platforms (e.g. Dropbox, OneDrive) without authorisation from Information Services. There are appropriate methods for storing draft and 'working' documents within the EDMS. Network drives are provided for non-corporate documents only and only limited quotas are allowed. It is the responsibility of each staff member to understand what documents should be stored in the EDMS, this information can be obtained from the Records Department.

2.2.5 Users will be responsible for any loss of data stored on local drives or on portable media.

2.2.6 Duplication of data is to be avoided. Any documents stored in the EDMS should not be stored elsewhere unless access to EDMS is planned to be unavailable or the data is stored on media specifically designed for the purpose of backup.

2.3 Installing Unauthorised Software or Files

2.3.1 Users must not purchase, install, copy or use any software without prior written consultation with Information Services.

2.3.2 The use of any files that are subject to Copyright regulations that have not been authorised in writing for use by the Copyright owner are not permitted to be used on the Shire systems.

2.4 Access to Computer Facilities

2.4.1 Users may use only those facilities to which they have been properly authorised to use by the relevant Manager/Director. Authorisation must be provided to Information Services in writing before access is provided and/or modified.

2.4.2 Users may not use any of the facilities provided by the Shire in such a way as to reflect poorly upon the Shire either in part or as a whole.

2.4.3 Users may not use any of the facilities provided to them by the Shire in such a way as to achieve personal gain or to earn income external to their employment at the Shire.

2.4.4 Where the use of any Information Services facility is governed by a password, the password must not be inappropriately divulged to any other person.

2.4.5 Any computer account or facility allocated to a user is for their exclusive use. The user must not allow another person to use it without appropriate authorisation from Information Services, Directors or the Chief Executive Officer (CEO).

2.4.6 Users will comply with any directive (verbal, written or electronic) from Information Services relating to access to Information Services facilities.

2.4.7 Any willful damage sustained to IT equipment will result in the costs of repair being sought from the user of the equipment. Any damage sustained to equipment as a result of neglect may result in the costs of repair or replacement being sought from the user of the equipment.

2.4.8 Users must be aware that the use of mobile computing facilities may result in significant communications costs. When users do not have access to local call connections to the Shire, on-line time should be kept to a minimum. The Shire will not be responsible for any excessive costs incurred. Mobile Broadband devices are available for specified staff, as approved by the CEO who have to travel and need internet access.

2.4.9 Information Services staff reserve the right to perform schedule and ad-hoc system maintenance tasks outside regular Administration Centre working hours. Where abnormal maintenance tasks are planned notification of the anticipated down time will be communicated if possible. If staff has a particular need for after hour's access to IT facilities they should liaise with Information Services staff in advance to arrange access options.

2.5 Security

2.5.1 Regardless of the prevailing security, or lack of security, users shall not access any data or software except data or software that belongs to the user or have been provided for their use, or is stored on a shared medium for which they have been granted access.

2.5.2 Users must not attempt to rename, delete, or modify the data of another user without prior authorisation from Information Services, except in the following circumstances:

2.5.2.1 For data or files stored on a shared network facility or transferred in/out via a shared network facility.

2.5.2.2 Under direction of their supervising officer(s) to amend data or files stored in a personal directory.

2.5.3 Anti-virus software protection is provided at both server and desktop level. If a user suspects that their machine has become infected with a virus (or similar type entity) it should be reported immediately to Information Services.

2.5.4 Users are encouraged to log out of their workstations when they are not in use. An auto-locking policy is in place that locks computers if not used for more than 15 minutes.

2.5.5 Users should correctly shut their computer systems down before finishing work each day, unless otherwise requested by Information Services.

2.5.6 Users must report to Information Services, without delay, any breaches (either real or perceived) of security.

2.5.7 Users must take every reasonable precaution to ensure that their passwords, accounts, software and data are adequately protected. The password should also meet complexity requirements and never be stored in plain text. A password manager should be used for this purpose (i.e. KeePass).

2.5.8 Users will be responsible for protecting company information from external threats by remaining vigilant and maintaining good cyber security awareness practice.

2.6 Voice Mail

2.6.1 Voice Mail is a corporate resource for business use and serves to provide a minimum level of customer service when a telephone is unattended. Where possible telephones should be diverted to another officer.

2.6.2 The legitimate use of Voice Mail is for cases where staff are out of their offices for short periods where phone calls would go unanswered. Voice Mail should not be used to take calls when staff are on leave.

2.6.3 Users must work with each other to minimise the reliance on Voice Mail as much as possible. This will serve to ensure that a high level of customer service is maintained.

2.7 IT Support

2.7.1 Requests for new systems will be formal and such requests will be treated in order of priority or in accordance with ~~a~~ directive from the Chief Executive Officer.

2.7.2 Information Services has an Electronic Helpdesk system which users should use to report problems or requests with, to Information Services. This system allows Information Services to attend to service calls in a fair sequence and by level of priority.

2.8 Internet and E-mail

2.8.1 E-mail users *must* delete any unnecessary messages promptly and manage their e-mail files wisely *to* ensure compliance with limits that are set on mailbox sizes; therefore, users should make sure e-mails are registered into the EDMS.

2.8.2 When commencing leave, staff should utilise the ability of the email software to forward incoming mail to the person who is acting in the position during their absence or set an out of office message.

2.8.3 Outlook Calendars are regarded as a management tool and should be made available for other staff to review. Personal appointments can be marked 'Private' so reviewers may not see the details of the content.

2.9 What is Acceptable Use in regards to Internet and E-mail?

2.9.1 Subject to the balance of this policy, employees may use the Internet access provided by the Shire for:

2.9.1.1 Work-related purposes.

2.9.1.2 Sending and receiving personal email messages, provided that if email messages are sent with a Shire of Murray email address in the from: or Reply -To: header, a disclaimer shall accompany the email to the effect that the views of the sender may not represent those of Shire.

2.9.1.3 Accessing the World Wide Web for limited personal purposes, provided in each case that the personal use is moderate in time, does not incur cost for the Shire and does not interfere with the employment duties of the employee or his or her colleagues.

2.9.1.4 Utilising any other Internet service or protocol for personal purposes after obtaining permission in writing, to do so, from the Shire's Information Services.

2.9.2 E-mail messages of a corporate nature that leave the Shire destined for an external organisation are public records and must be captured in the EDMS. Any corporate e-mail messages that officers receive must also be captured in this manner. If the user is unclear of how to capture the correspondence in the EDMS themselves such messages should be forwarded to Records staff to facilitate this legislative (*State Records Act 2000*) requirement.

2.10. What is Not Acceptable Use in regards to Internet and E-mail?

2.10.1 Except in the course of an employee's duties or with the express permission of the Shire, the Internet access provided by the Shire may not be used for:

2.10.1.1 Personal commercial purposes.

2.10.1.2 Sending unsolicited bulk email such as advertising or announcements that are not related to Council business to any group.

2.10.1.3 Sending any e-mail that is inappropriate, for example, e-mails that contains pornographic material, profanity, racial and sexual discrimination, forwarding of hoaxes, chain-mail, spam, harassing colleagues or knowingly sending or forwarding virus-infected e-mails.

2.10.1.4 Disseminating confidential information of the Shire.

2.10.1.5 Any illegal purpose.

2.10.1.6 Knowingly causing interference with or disruption to any network, information service, equipment or any user thereof.

2.10.1.7 Disseminating personal contact information of officers or employees of the Shire without their consent.

2.10.1.8 Knowingly causing any other person to view content which could render the Shire liable pursuant to equal opportunity or sexual discrimination legislation at the suit of that person; or

2.10.1.9 The use of real-time messaging services such as ICQ, MSN, Yahoo or similar programs.

2.10.1.10 Web sites including but not limited to those of the following nature:

- Adult Entertainment;
- Pornography; and
- Chat Rooms / Channels.

2.10.1.11 Reference the Shire of Murray Code of Conduct Local Government Employees and the Social Media Management Practice HR019 for information relating to accessing and using Social Media.

2.11 Example of Disclaimer to be used

This e-mail message, including any attached files, is private and may contain information that is confidential. Only the intended recipient may access or use it. If you are not the intended recipient please delete this e-mail and notify the sender promptly. The views of this sender may not represent those of the Shire. The Shire uses virus-scanning software but exclude all liability for viruses or similar defects in any attachment.

2.12 Consequences of Unacceptable Use

2.12.1 The Shire keeps and may monitor logs of Internet usage which may reveal information such as which Internet servers (including World Wide Web sites) have been accessed by employees, and the email addresses of those with whom they have communicated. The Shire will not, however, engage in real-time surveillance of Internet usage, will not monitor the content of email messages sent or received by its employees unless a copy of such message is sent or forwarded to the company by its recipient or sender in the ordinary way, and will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.

2.12.2 Responsibility for use of the Internet that does not comply with this policy lies with the employee so using it and such employee must indemnify the Shire for any direct loss and reasonably foreseeable consequential losses suffered by the Shire by reason of the breach of policy.

2.12.3 The Shire will review any alleged breach of this Acceptable Use Policy on an individual basis.

Policy Detail		
Responsible Directorate	Corporate Services	
Responsible Department	Information Services	
Responsible Officer	Manager Information Services	
Next Policy Review / Schedule	2026 (3-yearly)	
Council Adoption	**Date / Resolution**	23 April 2010 (OCM10/066)
Amendment Record	**Date / Resolution**	26 July 2012 (OCM12/149)
		25 July 2015 (OCM15/155)
		22 February 2018 (OCM18/008)
		19 December 2019 (OCM19/270)
		22 July 2021 (OCM21/114)
		23 June 2022 (OCM22/070)