Information Technology Security and Usage Policy

Policy	8C
Officer Responsible	Manager Information Technology
Last Review Date	21/11/2022

Strategic Policy

1. OBJECTIVE

The purpose of this policy is to outline the acceptable use of computer equipment at Blayney Shire Council and rules around security access to network resources. These rules are in place to protect the employees and Blayney Council. Inappropriate use exposes Blayney Council to risks including virus attacks, compromise of network systems and services and legal issues.

2. SCOPE

Internet/Intranet related systems, including but not limited to computer equipment, software operating systems, storage media, network accounts providing e-mail, Web browsing are the property of Blayney Shire Council. These systems are to be used for business purposes in serving the interests of Blayney Shire Council and our customers and community in the course of normal operations.

Information and/or data stored on Council's network and cloud are the property of Blayney Shire Council.

This policy applies to all employees, contractors, consultants and other workers at Blayney Shire Council including all personnel affiliate with third parties.

3. GENERAL USE AND OWNERSHIP

While Blayney Shire Council's network aims to provide a reasonable level of privacy, users should be aware that the data created on the corporate systems remains the property of Blayney Shire Council.

For security and network maintenance purposes, authorised individuals within Blayney Shire Council may monitor equipment, systems and network traffic at any time.

4. PASSWORD SECURITY

Authorised users are responsible for the security of their passwords and accounts. Authorised users can be held responsible for activities performed with user's credentials. Multi Factor Authentication will also be enabled on systems where possible.

The following password security rules shall apply:

- Passwords expire and must be changed after 60 days.
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length Uppercase characters (A through Z)
- Lowercase characters (a through z)
- A number (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- Last 2 passwords cannot be used

- Passwords are not to be shared with other staff. If a staff member needs to act in your role, then appropriate access will be granted to your own login for the duration of the acting period.

UNACCEPTABLE USE

Under no circumstances is an employee of Blayney Shire Council authorised to engage in any activity that is illegal under State or Federal legislation while utilising Blayney Shire Council owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use:

- Unauthorised copying of copyrighted material.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojans, malware)
- Using a Blayney Shire Council computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment workplaces laws.
- Sending unsolicited email messages including the sending of junk mail or other advertising material.
- Any form of harassment via email, whether through language, frequency or size of messages.
- Employees may not attribute personal statements, opinions or beliefs to Blayney Shire Council when engaged in blogging.
- Use of Council's IT resources for other than Council business which impedes Council business or incurs a cost to Council.

5. APPROVED SOFTWARE

No software shall be installed or purchased unless it has been approved by the Manager Information Technology for use on Council computers. Software will only be approved if Council has a current licence to install and use the software if:

- it is fit for the intended use;
- the procurement procedure has been followed; and
- it will not endanger network security and the software can be supported either internally and have support/contract arrangements with external vendors

6. EMAIL PRIVACY AND CONTENT

Email should not be considered a private or secured form of communication as it may be forwarded or read by a third party. Content of emails should be carefully considered before sending.

7. ACCESSING INFORMATION HELD IN PROTECTED DIRECTORIES AND MAILBOXES

In a situation where a staff member is unavailable and information is required from their mailbox or directories for which they have exclusive access, this information can be retrieved by IT Staff where:

- The need for the information is urgent and cannot wait for the availability of the authorised user; and
- A manager to whom the authorised user is responsible requests the information by email.

In a situation where the staff member is on extended leave and their email account needs monitoring, the IT Staff can provide access to their inbox to a designated Council officer following a written request via email from the relevant manager.

8. GRANTED ACCESS

Standard Access

Staff members shall be granted standard access to computer, network shares and resources. These include:

- Own Drive Access
- SharePoint Access
- Public folder access
- Staff Intranet
- Corporate software (based on model user if one)
- Other Council systems identified and approved by manager/director after completing IT New Starter Form
- No Access to install software on computers

Privileged (Administrator Access)

Privileged access shall be granted to staff that require special access to the network and other resources and requires approval from the relevant Director

These include:

- IT Staff
- Staff that require access to install software
- Domain Administrator Server Access
- Full Access to Corporate software; Business Paper software and Asset Management Software

9. NEW STAFF

An Employee IT Access Form is required to be completed and approved by the relevant department Director prior to Information Technology creating network access. Once the employee has commenced and inducted into the IT system the form will be sent to Human Resources for addition to the staff members' file.

10. DEPARTING EMPLOYEES

Upon a staff members departure the Information Technology department will fill in the Departing Employee IT Access Form. Once completed this will be sent to Human Resources to be added to the staff members' file.

11. CHANGE OF ROLE

Where a staff member changes roles, the Information Technology department must be informed by the Human Resources department. A Change of IT Access form will then be filled in and approved the relevant Director before changes are made.

12. ACTING IN A ROLE

Where a staff member is required to act in another staff member's role for a period of time, Information Technology must be informed by the staff members Director prior to the leave commencing so that appropriate access can be provisioned for the duration of the acting period.

End

Adopted:	**20/05/2019**	**1905/012**
Last Reviewed:	**20/05/2019**	**1905/012**
	21/11/2022	**2211/009**
Next Reviewed:	**18/11/2025**	