Somerset
REGIONAL COUNCIL

Policy Subject/Title: **Information Management and Security Policy**

Policy Number: **C015**

Responsible Officer:	Director Corporate and Community Services
Legislative References:	*Information Privacy Act 2009* *Local Government Act 2009* *Public Records Act 2023* *Right to Information Act 2009* Local Government Regulation 2009
Related Documents	F005 Risk Management Policy F012 Business Continuity Plan Policy HR001 Code of Conduct Code of Conduct for Councillors in Queensland C020 Social Media Policy – Guidelines for Use C021 Style Guide Policy Essential 8 Framework and Information Security Manual: Australian Signals Directorate, Cyber Security Terminology < Cyber Security Terminology | Cyber.gov.au > National Institute of Standards and Technology, US Department of Commerce, Computer Security Resource Centre 'Glossary' < Glossary | CSRC (nist.gov) > Queensland Government's Information Security Standard (IS18:2018) Queensland State Archives: Records governance policy v1.0.2 Queensland State Archives: Records governance policy implementation guideline v1.0.1

Related Forms:	*Right to Information and Information Privacy Access Application* CCTV Information Request Form (F563) Employee Permissions (F841)
Authorised by:	Somerset Regional Council
Authorised on:	27 November 2024 (Doc Id 1688953, 1689023)
Effective date:	5 December 2024
Review / Amendment dates:	

CONTENTS

1. PURPOSE

The purpose of this policy is to:

- transform information management from an operational function to a strategic enabler, supported at all levels of Council and
- document Council's commitment to take all reasonable steps to ensure:

    - the integrity and completeness of information being made, managed and preserved by Council[1];
    - a strong foundation for systematically and effectively managing complete and reliable records and information[2];
    - the security of confidential information held by Council;
    - the protection of personal information collected, stored, handled, accessed, amended, managed, transferred, used or disclosed by Council[3].
    - the discoverability and accessibility of records and information[4];
    - compliance with requests to access records in accordance with the provisions of the *Right to Information Act 2009*, the *Information Privacy Act 2009* and by Court Order;
    - a consistent approach to the implementation of information security to protect *Corporate Information*, information assets and associated physical assets against unauthorised use or accidental modification, loss or release; and
    - maintaining business continuity.

2. SCOPE

This policy applies to all *Corporate Information*, including, but not limited to, *Public Records*, *Confidential Information*, and *Personal Information*. All *Elected Members* and *Staff* must comply with this policy.

As members of a *Public Authority*[5], all *Elected Members* and *Staff* have a responsibility to make and manage full and accurate records of Council actions or decisions[6] and actively support compliance with Queensland State Archives Records Governance Policy requirements[7].

All *Elected Members* and *Staff* are also responsible for protecting information held by Council. This protection includes:

- not releasing information that the *Elected Members* and *Staff* know, or ought reasonably to know, is *Confidential Information*[8]*;*
- not using *Confidential Information* to gain an advantage (personally or for someone else) or to cause detriment to the local government[9];
- not disclosing *Personal Information* unless allowable by the *Information Privacy Principles* or other relevant legislation
- maintaining and promoting a culture of information security to protect *Corporate Information.*

---

[1] Schedule 1 'Public record principles', *Public Records Act 2023*.
[2] Queensland State Archives: Records governance policy v1.0.2, p. 1.
[3] s6, *Information Privacy Act 2009.*
[4] Queensland State Archives: Records governance policy v1.0.2, p. 1.
[5] s8, *Public Records Act 2023.*
[6] Part 2, Division 2, *Public Records Act 2023.*
[7] Queensland State Archives: Records governance policy v1.0.2; Queensland State Archives: Records governance policy implementation guideline v1.0.1.
[8] s171, *Local Government Act 2009;* s200 *Local Government Act 2009.*
[9] s171, *Local Government Act 2009;* s200 *Local Government Act 2009.*

The responsibility to protect *Confidential Information* and *Personal Information* remains in effect even when *Elected Members* or *Staff* cease their role with Somerset Regional Council.

Individual responsibilities include, but are not limited to:

- being aware of *Corporate Information Systems*
- being competent in the use of Council's *Electronic Document Records Management System* (*EDRMS*), if you have authorised access to this system;
- ensuring all documents created or that need to be created by the individual are registered in Council's *Electronic Document Records Management System* (*EDRMS*);
- only viewing or retrieving *Corporate Information, Confidential Information* and *Personal Information*, and any other resources that are required for the functioning of their position
- protecting information held by Council, including *Corporate Information, Public Records*, *Confidential Information* and *Personal Information*,
- protecting information that could identify an individual,
- ensuring cyber security measures are complied with,
- attending appropriate training courses provided, and asking for assistance when needed, either for training or system related problems;
- complying with all policies and procedures that relate to the management of *Corporate Information*.

Third Party Providers are also responsible for protecting *Corporate Information*, *Confidential Information* and *Personal Information.* All reasonable steps will be taken to protect information Council holds from loss, unauthorised access, use, modification, disclosure or any other misuse. This includes taking all reasonable steps to prevent unauthorised use by contractors engaged for the provision of a service to Council.

3. DEFINITIONS

a)	*Access*	means providing an individual with personal information about himself / herself that is held by Council. This may include allowing that individual to inspect personal information or to obtain a copy of the personal information.
b)	*Associated Document*	*Corporate Information* that relates to the same topic or task
c)	*Authorised Individual/s*	a named individual who has been explicitly granted permission to use a system, application, resource or facility.
d)	*Authorised Person/s*	an individual appointed in order to investigate, monitor and enforce compliance with various legislation within the parameters of a local government.
e)	*Confidential Information*	is information generally not known by or available upon request to the public. This includes information that: - identifies and relates to a particular individual, or - carries a risk that, if released or improperly used, would cause harm to the Council or a member of the community, or give an unfair advantage to someone.

For clarity, the following classes of information must always be treated as confidential:

(i) legal advice received by Council, including the request for legal advice, the substance or effect of that legal advice, or any conclusions reached in that legal advice, or any reasoning upon which those conclusions were reached, or any course of action recommend in that legal advice;

(ii) information provided to Council on the condition that it is kept confidential;

(iii) information dealing with the appointment, dismissal, discipline or appraisal of employees;

(iv) information dealing with industrial matters affecting employees;

(v) information associated with the preliminary budget;

(vi) information dealing with rating concessions;

(vii) information associated with contracts proposed by the Council;

(viii) information associated with starting or defending legal proceedings;

(ix) information dealing with the security of property;

(x) information dealing with trade secrets of any person or body;

(xi) information considered and discussed in meetings closed to the public, pursuant to the *Local Government Act 2009* and Local Government Regulation 2012[10];

(xii) commercial-in-confidence information associated with any person or body;

(xiii) names and / or addresses of complainants or witnesses; or

(xiv) any other information designated as confidential by the Chief Executive Officer, unless Council resolves otherwise. For example, a report is presented to Council

[10] s254J Local Government Regulation 2012.

		designated as Confidential by the CEO, Council can then read the agenda and make a determination as to whether it is confidential or not. Council can resolve THAT this matter be discussed in open session and / or the confidentiality designation for this matter be removed / direct CEO to remove the confidential designation on this matter.
f)	*Corporate Information*	includes, but is not limited to, *Public Record*/s, discussions, documents, electronic data or knowledge.
g)	*Corporate Information Systems*	Any software, programs or platforms utilised by *Elected Members* and *Staff* including, but not limited to Skytrust, Onedrive, Sharepoint, Reflect, Civica Practical, Guardian, etc. that contain *Corporate Information*.
h)	*Corporate Social Media Accounts*	includes the Somerset Regional Council Facebook page, Instagram and LinkedIn accounts.
i)	*Corporate Website*	means < www.somerset.qld.gov.au >
j)	*Cyber Security Event/s*	an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
k)	*Cyber Security Incident/s*	an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations.
l)	*Data Owner*	is accountable for specified Council activities and may also be responsible for those activities on a day to day basis individually, or with the assistance of other *Authorised Individual/s* (as specified in Clause 4.4.1 of this policy).
m)	*Data Breach*	any kind of unauthorised access, disclosure or loss of *Personal Information.*
n)	*Disciplinary Action*	may include: - suspension, disconnection or cancellation of access to *Systems* (all or part) either permanently or on a temporary basis, - issuing a warning, - termination of employment, - termination or non-renewal of contractual arrangement, - civil or criminal liability and / or prosecution.

o)	*Elected Members*	the Mayor, Deputy Mayor and Councillors.
p)	*Electronic Document Records Management System* or *EDRMS*	is MAGIQ Documents software. All other *Corporate Information Systems* utilised by Council are not Council's *Electronic Document Records Management System*.
q)	*Ephemeral Documents*	emails that are not *Public Records*, have short term informational value and are only required to be retained for a short time (while they are needed for reference purposes). Examples of *Ephemeral Documents* include: - duplicate or cc (courtesy copy) emails that are used only for reference or information purposes and not as a public record - emails that are part of a distribution list - meeting / appointment notifications - spam and unsolicited advertising material - out of office notifications - automated replies.
r)	*Financial Management System*	is Civica Practical. All other *Corporate Information Systems* utilised by Council are not Council's *Financial Management System*.
s)	*Group Membership*	a method of providing the same access permission to a defined group of *Authorised Individuals*. Membership of each defined group is specified in C015 – P01 ICT Management and Security Procedure.
t)	*ICT*	Information Communication Technology
u)	*Information Privacy Principles*	as outlined in Schedule 3 'Information privacy principles' of the *Information Privacy Act 2009*[11].
v)	*Least Privilege*	information security concept promoting minimal user profile privileges based on the task necessities of an *Authorised Individual* in the context of their appointed role.
w)	*Need To Know*	information access controls that deny access by default unless explicitly authorised by the *Data Owner*.
x)	*Non-Corporate Websites*	means other than Council's *Corporate Website* e.g. < www.experiencesomerset.com.au >. Responsibility for *Non-Corporate Websites* is with the relevant section's Manager or Team Leader.

[11] Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

y) *Personal Information* — as per definition in the *Information Privacy Act 2009*[12].

Note that the definition of 'individual' in the Acts Interpretation Act 1954 (Qld) is 'a natural person'[13]. A natural person can only be a living person, however care should be taken when handling information of the deceased, as it may also be personal information of the living, for example, a family member.

Types of personal information held by Council may include, but are not limited to:

- names and addresses
- telephone numbers
- age and/or date of birth
- property ownership and/or occupier details
- animal ownership
- payment histories
- pensioner/concession details
- library membership
- photograph/s or other pictorial representation of a person.

Documents to which the *Information Privacy Principles* do not apply include, but are not limited to:

- generally available publications, for example, White Pages Australia directory; information or documents available on readily available websites;
- anything kept in a library, art gallery or museum for the purpose of reference, study or exhibition;
- material kept in public records and archives such as the Commonwealth or State archives that is not in a restricted access period under the *Information Privacy Act 2009*;
- those contained in a public interest disclosure;
- those relevant to an investigation into corruption.[14]

z) *Privacy Officer* — the Director Human Resources and Customer Service and the Director Corporate and Community Services.

aa) *Privileged Access* — is access by an *Authorised Individual* that has permission to:

- make changes at an administrator level, and / or
- access higher security areas restricted to specified *Authorised Individuals*.

[12] Definition of 'Personal Information', Schedule 5 Dictionary, *Information Privacy Act 2009*; s12 *Information Privacy Act 2009*.
[13] Schedule 1 Meaning of commonly used words and expressions, *Acts Interpretation Act 1954*.
[14] Schedule 1 Documents to which the privacy principles do not apply, *Information Privacy Act 2009*.

bb) *Public Authority* — as per definition in the *Public Records Act 2023*[15].

cc) *Public Record/s* — as per definition in the *Public Records Act 2023*[16].

As further guidance, a *Public Record* is any document that meets one or more of the following criteria:

- Does it provide evidence of the actions and / or decisions of a *Public Authority* while undertaking its activities (e.g. exercise of its statutory, administrative or other public responsibilities)?
- Does it provide context to a *Public Record*?
- Does it convey information essential or relevant in making a decision?
- Does it convey information upon which others will be, or are likely to be making decisions affecting the Council's operations, or rights and obligations under legislation? e.g. does it document advice given or received in the course of business.
- Does it commit Council to certain causes of action or the commitment of resources or provision of services? e.g. does it document a business decision.
- Does it provide evidence of a business transaction?
- Does it convey information about matters of public safety or public interest, or involve information upon which contractual undertakings are entered into?
- Is the information likely to be needed for future use, or is it of historical value or interest?

Public Records are based on content (what is being documented), not the format used or where they are located (e.g. *Corporate Information Systems,* social media accounts, mobile devices, non-Corporate email accounts, etc.).

The term includes, but is not limited to:

- emails, texts and instant messages
- incoming correspondence
- outgoing correspondence
- timesheets
- telephone conversations
- financial transactions
- internal documents and correspondence (e.g. maps, plans, drawings, photographs, reports,

[15] s8, *Public Records Act 2023*.
[16] s9, *Public Records Act 2023*.

memos)
- inspection reports
- warranty documents
- file notes
- files
- social media posts, comments and messages
- videos and body worn camera footage
- data and content produced in software.

dd) *Software Liaison/s* — includes all staff who hold a nominated role in Council's organisational structure and are listed as a *Software Liaison* for a specified *Corporate Information System* in C015 – P02 Records Management and Security Procedure.

ee) *Staff* — includes a person employed by Somerset Regional Council on a temporary, part-time or full-time basis and, also, includes a person engaged to perform standard employee functions under a contract for services (e.g. contractor, consultant, etc.).

ff) *System/s* — includes anything that stores, transmits, or processes digital information, including but not limited to:

- any Council issued *ICT* equipment e.g. computers, tablets, phones, printers, scanners, etc.
- computer programs
- software applications
- cloud-based applications
- closed circuit television (CCTV) system.

gg) *Third Party Providers* — service providers, integrators, vendors, telecommunications and infrastructure support that are external to the organisation.[17]

4. POLICY

4.1 PROPER MANAGEMENT OF PUBLIC RECORDS

4.1.1 What is a Public Record?

The definitions section of this policy provides useful guidance on what constitutes a *Public Record* for the purposes of this policy.

Failure to adequately keep records in Council's *Electronic Document Records Management System* (*EDRMS*) may result in *Disciplinary Action* and could leave individuals at risk of prosecution for unlawful disposal of public records[18]. Disposing of a public record includes,

[17] 'Third-party Providers – Glossary', National Institute of Standards and Technology < Third-party Providers - Glossary | CSRC (nist.gov) >.
[18] s23 *Public Records Act 2023*.

but is not limited to, destroying, deleting, altering or damaging a record in such a way that the accuracy and / or integrity of the record is compromised.[19]

The accepted process for dealing with a *Public Record* is outlined in this policy. Advice about the proper document management process applicable to a *Public Record*, other than those provided in this policy, should be directly sought from C015 – P02 Records Management and Security Procedure or Council's Records Team.

- **Emails, texts and instant messages**
  Staff, and *Elected Members*, receiving and sending business related emails, texts and instant messages are responsible for ensuring that all details are registered in Council's *EDRMS* in accordance with instructions provided in C015 – P02 Records Management and Security Procedure. This includes emails, texts and instant messages relating to Council business received to a non-Corporate email account, phone or instant message service.

  Emails that are not *Public Records*, have short term informational value and are only required to be retained for a short time (while they are needed for reference purposes) are referred to as *Ephemeral Documents. Ephemeral Documents* are not required to be registered in Council's *EDRMS* because they do not meet the definition of a *Public Record.*

  The use of non-Corporate email accounts when conducting official Council business is prohibited and could result in *Disciplinary Action*. Should an email relating to official Council business be received to a non-Corporate account, the receiver should respond to the sender and direct them to use the Council issued email address (the Councillor's official Somerset Regional Council issued email address, or for staff, < mail@somerset.qld.gov.au >).

  The use of social media platforms to conduct official Council business where settings enable messages to be deleted / removed upon opening / being read in the first instance is prohibited and could result in *Disciplinary Action*. Examples of these platforms include, but is not limited to, Snapchat and WhatsApp. The use of social media platforms where messages can be removed instantaneously (or close to) creates an unreasonable risk to the loss and destruction of *Public Records*.

- **Incoming Correspondence**
  Incoming correspondence will be registered in Council's *EDRMS* by the Records Team and forwarded to the responsible officer. Documents will be distributed via the responsible officer's Task List for appropriate action. It is every officer's responsibility to check their task list on a regular basis.

  Exceptions to electronic distribution will be:

  - documents containing pages larger than A3 in size;
  - hard copied items that cannot be scanned (books, annual reports, etc.)
  - forms, surveys and other documents that require signatures or items to be filled out by the Council or a representative.

- **Outgoing Correspondence**
  Staff and *Elected Members* producing outgoing correspondence will be responsible for ensuring that the correspondence is registered in Council's *EDRMS* in accordance with C015 – P02 Records Management and Security Procedure.

[19] see definition of 'dispose' in Schedule 3 'Dictionary', *Public Records Act 2023*.

Physical outgoing correspondence (hard copy) that:

- is a *Public Record*,
- is not registered electronically,
- does not have a digital signature applied, and
- contains a signature that needs to be documented in Council's *EDRMS,*

must be left with an appropriately sized and addressed envelope in the Outgoing Mail tray located in the vicinity of the Records Team for scanning and registration into Council's *EDRMS*. After scanning and registering, the Records Team will seal the hard copy documents in the addressed envelope provided in readiness for the Customer Service Team to complete the outgoing mail process.

- **Timesheets**
  All timesheets will be recorded accurately into Council's *Financial Management System* by relevant officers. These officers will be responsible for inputting the information as provided and will not be responsible for any inaccurate or incomplete information so provided.

- **Telephone Conversations**
  Notes concerning business related telephone conversations are to be entered in Council's *EDRMS* if considered appropriate by the *Elected Member* or *Staff* engaged in the relevant conversation. Accountability for this requirement rests solely with the *Elected Member* or *Staff* member involved in the conversation. If the conversation is integral to a decision making process, it is appropriate that it be captured. Recordings of conversations are to be treated in the same manner.

- **Financial Transactions**
  All financial transactions of the Council are to be recorded in the *Financial Management System*.

- **Internal Documents and Correspondence**
  All internal correspondence, including email correspondence, is to be dealt with in the same manner as external correspondence and registered in Council's *EDRMS* if it is a *Public Record*.

  For Officer's Reports, the final version is the version of document considered by Council at its meeting, albeit that this may be different to the version submitted by *Staff* for the draft agenda. Council's meeting agenda, being the final version as distributed to Councillors for consideration, is registered as a document, in its entirety.

- **Inspection Reports**
  All versions of inspection reports are to be maintained and registered in Council's *EDRMS*.

- **Warranty documents**
  Warranty documents will be captured in Council's *EDRMS* under a specific warranties folder and once captured, are to be assigned as tasks to the most relevant officer (e.g. the workshop supervisor for mobile plant warranties) to manage the risk of Council commissioning maintenance over an item that is covered by warranty.

- **File Notes**
  File notes, including hand written notes, must also be entered into Council's *EDRMS*.

- **Files**
  Staff that borrow files accept responsibility for the location and security of those files until they are returned to the Records Team. Files must be returned to the Records Team when no longer required. If a file is passed from one *Staff* member to another, it is the responsibility of the first *Staff* member to notify the Records Team of the changing location.

- **Social Media Posts**
  It is acknowledged that social media is a tool used by both *Elected Members* and *Staff to* promote Council and its activities. Social media posts that are a direct share of material prepared and posted by *Staff* are not required to be registered, as these will be captured in Council's *EDRMS* by the *Staff* member who has produced and sought approval for public release of the material.

  Staff and *Elected Members* making social media posts that relate to Council business and activities, other than reposting of material prepared and posted by *Staff*, are responsible for ensuring that details are registered in Council's *EDRMS*, if they meet the definition of a *Public Record.* This includes any comments made on social media posts, unless the comment is simply tagging another social media user with no other comment or wording. A screenshot of the post and / or comment is sufficient.

  Elected Members and *Staff* should encourage members of the public to use email for Council matters due to the benefits of record keeping and the potential to provide a considered response where necessary.

- **Videos and body worn camera footage**
  Staff that produce videos or body worn camera footage are responsible for ensuring that C015 – P04 Body Worn Camera and Recording Phone Calls Procedure is adhered to.

- **Data produced in software (e.g. Skytrust, Reflect, Civica Practical, etc.)**
  Software Liaisons are responsible for ensuring that the data and content in *Corporate Information Systems* is registered into Council's *EDRMS*.

  Software Liaisons are also responsible for compliance with requests to access records in accordance with the provisions of the *Right to Information Act 2009*, the *Information Privacy Act 2009* and by Court Order.

4.1.2 Creating and Registering a Public Record

Public Records require all necessary details for a record to be full and accurate, including all attachments. This means that any *Public Record* must contain content, context and have a structure.

To create a full and accurate *Public Record*:

- Ensure the subject line is a summary of the document or an action statement. It may also contain a file reference or a document identification number for the document attached or an *Associated Document*.

- Include a signature or salutation block.

- If sending an email, include a disclaimer concerning dissemination or distribution of contents to / by unintended recipients.

To ensure information security and business continuity, when creating and registering *Public Records*, the following action must be taken:

- All internally and externally created emails that are identified as *Public Records* should be captured in Council's *EDRMS* as soon as possible, and within two (2) business days. Once the email has been captured in Council's *EDRMS,* it should be deleted from the *Authorised Individual's* email account.

  If there is uncertainty or confusion about whether an email is a *Public Record*, or whether it can be deleted or not, the Records Team should be consulted.

- If sending an email external to the organisation (someone other than *Elected Members* or *Staff*), Council's corporate email address should be used: < mail@somerset.qld.gov.au >, External emails should be received via Council's corporate email address < mail@somerset.qld.gov.au >, not the email address issued to an *Authorised Individual*. Failure to do so may result in *Disciplinary Action*.

- When sending an email to multiple recipients and at least one of these is external to the organisation, the BCC (blind carbon copy) option should be used to protect the privacy of the recipients, and Council's individually issued email addresses. This negates the possibility of external parties emailing a *Staff* member directly, instead of through < mail@somerset.qld.gov.au > as required by this policy.

- Email threads (a series of replies back and forth pertaining to the same message) are to be captured as each email is sent or received. As capture becomes a routine component of the business process, the risk of non-capture of records is reduced.

- External emails, being those received from people other than *Elected Members* and *Staff*, are to be registered by Council's Records Team. These emails should be received via Council's corporate email address: < mail@somerset.qld.gov.au >.

- For internal emails (emails sent between *Staff*), it is the responsibility of the sender to register the email in Council's *EDRMS*. Should the recipient of an internal email respond, the recipient becomes the sender and is therefore responsible for registering the response in Council's *EDRMS.*

- Should *Elected Members* send or receive *Public Records* via email, they are required to forward or bcc (blind carbon copy) < mail@somerset.qld.gov.au > to enable the Records Team to capture the records in Council's *EDRMS*.

- *Staff* who have been granted an exemption by the Chief Executive Officer to specified requirements contained within this policy are listed in C015 – P02 Records Management and Security Procedure, along with:

  - the specific requirements they are exempted from, and
  - the alternative process they are required to follow.

4.1.3 Amendments to Public Records

Any amendments made to Council information must be auditable. Audit trail requirements include:

- Date of amendment

- Reason for amendment
- *Staff* member responsible for amendment
- Authority for amendment
- Notification of stakeholders of information (if appropriate).

Emails assessed as *Public Records* cannot be altered after they have been sent or received. If an email that is a *Public Record* is forwarded or amended and sent to someone else in the course of business, it must be captured as a new *Public Record*.

4.1.4 Retention and Disposal of Public Records

All *Public Records* will be retained and disposed of in accordance with the approved Queensland State Archives Retention and Disposal Schedules. Details of the Schedules are available by contacting the Records Team.

Elected Members and *Staff* are not to dispose of *Public Records*. The disposal of documentation will be carried out by the Records Team and *Software Liaisons*, at the direction of the Chief Executive Officer.

It should be noted that once a document is registered into Council's *EDRMS*, the copy of the registered document stored in a Council *System* should be deleted.

4.1.5 Software Liaisons

Staff appointed to a Director role and *Software Liaisons* are responsible for ensuring that:

- the data and content in *Corporate Information Systems* is registered into Council's *EDRMS*
- only appropriate and approved documentation or data is captured in *Corporate Information Systems* e.g. copies of photographic identification is not to be recorded in Council's *Corporate Information Systems*.

Software Liaisons are staff who hold a nominated role in Council's organisational structure and are listed as a *Software Liaison* for a specified *Corporate Information System*. They are required to be:

- a regular user of the *Corporate Information System* for which they are appointed,
- well versed in its use and capacity, and
- capable of providing training to relevant *Staff* in the use of the *Corporate Information System*.

Further guidance relating to the *Software Liaisons'* role and the appointment process is contained within C015 – P02 Records Management and Security Procedure.

Upon receipt of requests for *Public Records* (e.g. Right to Information applications, Information Privacy Applications, Court Orders), *Software Liaisons* are responsible for:

- searching *Corporate Information Systems* for requested documents,
- auditing documents found matching the search criteria to ensure they are registered in Council's *EDRMS,* and
- providing a signed memorandum to the Director Corporate and Community Services and the Records Team Leader, advising the extent of the search undertaken, the results of the audit and attaching a schedule of documents.

Software Liaisons are responsible for disposing of copies of *Public Records* held in *Corporate Information Systems*, other than Council's *EDRMS,* consistent with Council's retention and disposal schedule, at the direction of the Chief Executive Officer.

It should be noted that for business continuity purposes, all *Corporate Information Systems* and *Systems* must have a member of the Information Services Team nominated as an administrator.

4.1.6 Security and Monitoring

Software Liaisons designated for *Corporate Information Systems* in accordance with C015 – P02 Records Management and Security Procedure, are responsible for ensuring that adequate training is available to all *Staff*, both at induction and on an ongoing basis, to ensure *Staff* capabilities are sufficient to meet their responsibilities.

Software Liaisons will be responsible for auditing staff capabilities on a quarterly basis. This may take the form of auditing the data and content contained in a *Corporate Information System* with that registered in Council's *EDRMS*, or undertaking any other relevant means of testing the security and accuracy of Council's *Corporate Information* and *Systems*. This testing may be conducted for all *Authorised Individuals* or selected *Authorised Individuals* (including by random selection).

Audit results will be recorded on employee personnel files in Council's *Electronic Document Records Management System*. The outcome of auditing will help inform Council's cybersecurity and record keeping strategies, including whether additional training is required, and the main sources / areas of risk. Unsatisfactory audit results, demonstrated on three (3) occasions, may result in *Disciplinary Action* and additional controls being implemented for relevant *Systems*.

Software Liaisons will report to their Director, the Chief Executive Officer and the Manager Information Services when the actions of an *Elected Member*, *Staff* member or *Authorised Individual* have breached, or are suspected to have breached, this policy and / or any other Council policies or procedures.

If *Software Liaisons* have concerns about staff capabilities at any time, especially post-audit, they must raise this with their Director, the Chief Executive Officer and the Manager Information Services.

4.1.7 Exit Process

It is the responsibility of the *Elected Member* or *Staff* member exiting the organisation to ensure that any work product contained in Council's *Systems* is dealt with appropriately. This may include, but is not limited to:

- ensuring all *Public Records* have been registered into Council's *EDRMS;*
- *Public Records* that have been registered into Council's *EDRMS* have been deleted from the *System* in which they were originally created / stored;
- draft documents that do not constitute a *Public Record* are deleted;
- position manuals / instructions / proforma documents updated and supervisor notified of their location.

Should the *Elected Member* or *Staff* member fail to complete this process, the responsibility for undertaking the required tasks will fall to the *Software Liaison*, in the event it is an *Elected Member*, or the *Staff* member's supervisor, should it be a member of *Staff*.

4.2 PROPER MANAGEMENT OF CONFIDENTIAL AND PERSONAL INFORMATION

4.2.1 How is *Confidential Information* to be treated?

Elected Members and *Staff* will preserve the confidentiality of *Confidential Information*, to the fullest extent possible. *Confidential Information* will only be released when Council is obliged to do so in accordance with relevant legislative provisions.

Confidential Information must not be released to any person unless:

- the information relates only to that person (i.e. it is solely information about the person); or
- it is information that relates to a person, and that person has provided Council with written authority to release the information to someone else; or
- the release is necessary for the conduct of Council's business and is in the public interest; or
- the Council is obliged by law to release the information to that person.

If *Elected Members* or *Staff* are unsure whether information or a document is confidential, the *Elected Members* or *Staff* must consult with the Chief Executive Officer (or the Chief Executive Officer's delegate) before taking any action that may result in the information or document becoming available to a member of the public.

Elected Members and *Staff* must not access *Corporate Information* except to the extent that it is necessary to do so in order to perform official duties.

Failure to protect *Confidential Information* will result in *Disciplinary Action* and could leave individuals at risk of prosecution for:

- releasing information that *Elected Members* or *Staff* know, or ought reasonably to know, is *Confidential Information*,
- using *Confidential Information* acquired as *Elected Members* or *Staff* to gain an advantage (personally or for someone else),
- using *Confidential Information* acquired as *Elected Members* or *Staff* to cause detriment to the local government.[20]

The responsibility to protect *Confidential Information* remains in effect even when *Elected Members* or *Staff* cease their role with Somerset Regional Council.[21]

4.2.2 How is *Personal Information* to be treated?

Personal Information is to be treated in accordance with the *Information Privacy Act 2009* and the *Information Privacy Principles*[22] contained therein.

All personal information collected by Council will only be used for the purpose of conducting Council business and for the provision of services to the community. Personal information sought by Council will be the minimum required to undertake Council business e.g. identifying the personal information needed to do our job, and limiting the collection of personal information to only that.

Council will not retain copies of identification documents (e.g. drivers licences, pensioner cards, etc.) once they have been sighted by the relevant *Staff* member to verify a person's identity, unless there is a legislated or internal control reason for doing so. This includes

[20] s171, *Local Government Act 2009*; s200 *Local Government Act 2009*.
[21] s171, *Local Government Act 2009*; s200 *Local Government Act 2009*.
[22] Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

identification documents belonging to *Elected Members*, *Staff*, customers and any other individual that may have business dealings with Council. Further instructions relating to the management of identification documents can be found in Council's C015 – P02 Records Management and Security Procedure.

An individual may make a written request to access their own personal information by completing a 'Right to Information and Information Privacy Access Application'. Suitable photographic identification must be sighted by the relevant *Staff* member, prior to an individual accessing the documents requested (i.e. drivers licence, passport, 18+ card).

Council will not disclose personal information to a person, body or agency (other than the individual concerned) unless:

- the disclosure is for the purpose of distributing materials for and on behalf of Council, or when a third party has been contracted by Council, for the sole purpose of assisting Council in providing services to the community;
- for the purpose of validating information in databases held by other Government entities or agencies;
- the requirements of Clause 11 of the *Information Privacy Principles* have been met[23].

Council must take all reasonable steps to ensure that the person, body or agency to which personal information is disclosed to does not use or disclose the information for a purpose other than the purpose for which it was given[24].

Should personal information be disclosed by Council for a purpose outlined in Section 11(1)(e) of the *Information Privacy Principles*, Council must include with the document, a note of disclosure[25]. This will include details about what was disclosed, and to whom.

4.2.3 Closed Circuit Television (CCTV) Cameras, Body Worn Cameras and Vehicle Mounted Cameras (Dash Cam)

Council strives to provide a safe and secure environment for residents, visitors and *Staff*. Council has installed a number of cameras for security, public safety, crime prevention and verification purposes.

Closed circuit television (CCTV) refers to the use of CCTV cameras to capture and transmit a signal to a specific place. These cameras may be fixed or may be mobile.

Any proposed new fixed CCTV camera positions, or changes to existing fixed CCTV camera positions, will require a resolution of Council prior to installation or the proposed changes being made. However, fixed CCTV cameras proposed to be installed inside a Council facility are approved by the Chief Executive Officer. Careful consideration must be given to whether the *Personal Information* collected:

- directly relates to a function of Council,
- what the CCTV camera surveillance is intended to achieve,
- whether installation is necessary to achieve this purpose
- whether there is an alternative strategy to achieve the purpose[26].

Fixed CCTV cameras are usually installed for security and public safety purposes.

---

[23] Schedule 3 Information privacy principles, *Information Privacy Act 2009*.
[24] s11(3), Schedule 3 Information privacy principles, *Information Privacy Act 2009*.
[25] s11(2), Schedule 3 Information privacy principles, *Information Privacy Act 2009*.
[26] IPP1, Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

Council controlled CCTV will:

- be affordable to the community, but provide an effective service;
- be a reactive system based on retrieval of historical imagery or recordings, with no active overwatch of current images, video or other data (with the exception of flood cameras, which are readily accessible from Council's Disaster Portal in real time);
- provide information about weather events;
- be used to identify, manage, deter and reduce criminal behaviour, particularly in respect of Council resources;
- assist police in obtaining evidence to prosecute criminal offences
- verify a sequence of events
- be located at a site that ensures collection of information is not unnecessarily intrusive and will best achieve the purpose of the collection.

Elected Members, *Staff* and visitors in the vicinity of Council facilities are likely to have their image and voice captured on Council's CCTV system, which may be monitored and retained in accordance with this policy. Council gives no warranty or assurance about the confidentiality or privacy of any *Personal Information* disclosed whilst using *Corporate Information Systems* for personal purposes, or when using Council *Systems* or personally owned devices in the vicinity of Council's CCTV system.

Body Worn Cameras will be used by *Authorised Persons*, at present limited to the Regulatory Services Team, to:

- provide a visual deterrent to moderate aggressive behaviours by persons towards *Authorised Persons;*
- inspire professional conduct by *Authorised Persons;*
- improve collection of evidence;
- reduce administrative reviews, decisions and complaints against *Authorised Persons;*
- minimise errors, mistake of fact and improve successful resolution of matters; and
- improve administrative efficiency allowing for increased field time and better engagement addressing customer requests.

Similarly, Vehicle Mounted Cameras (Dash Cam) will be used by *Authorised Individuals* to undertake tasks including, but not limited to:

- verifying delivery of notices
- auditing of roads, signage and to undertake rumble tests.

While CCTV cameras are placed so as not to be unnecessarily intrusive, body-worn cameras and vehicle mounted cameras by necessity travel with relevant *Staff*, partly for the protection of the *Staff.* To negate the risk of these cameras being unnecessarily intrusive, *Authorised Persons* are required to comply with the provisions contained within C015 – P04 Body Worn Camera and Recording Phone Calls Procedure.

Collection of Personal Information

Council will only collect *Personal Information* where it is for a lawful purpose and the purpose of collection directly relates to fulfilling a function or activity of Council[27]. For clarity, when Council controlled cameras record an image or voice, it is recording *Personal Information*.

[27] IPP1, Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

Council will advise the public both on its website and on collection notices in the vicinity of CCTV cameras, why it is collecting information and to whom it intends to provide the information[28].

Council are not required to display collection notices in the vicinity of Body Worn Cameras, as exemptions to the Information Privacy Principles apply when undertaking functions or activities as an enforcement agency.[29] For clarity, Council, as an enforcement agency, is not subject to Information Privacy Principles 2, 3, 9, 10 or 11 when undertaking functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed.[30]

Council will treat the *Personal Information* collected by Council controlled CCTV, including images and sound, in accordance with Clause 4.2.2 of this policy, the *Information Privacy Act 2009* and the *Information Privacy Principles*[31] contained therein. The collection of *Personal Information* will be undertaken by:

- an *Authorised Individual* engaged in monitoring the CCTV footage, and tasked with accessing and downloading *Personal Information* (i.e. video images), when required; or
- an *Authorised Person* issued with a body worn camera or an *Authorised Individual* issued with a vehicle mounted camera, who will access and download *Personal Information* (i.e. video images), when required.

Council will make best endeavours to ensure the *Personal Information* has accurate meta data recorded with the footage where possible (including date and time).

Storage, Retention and Disposal of Personal Information

Any *Personal Information* that is captured by Closed Circuit Television (CCTV) Cameras, Body Worn Cameras and Vehicle Mounted Cameras (Dash Cam) must be adequately protected against misuse, loss, unauthorised access and disclosure[32]. This means protecting both the stored camera footage and cameras when surveillance monitoring takes place.

Storage, retention and disposal of *Personal Information* will be managed in accordance with this policy and its Related Documents.

It should be noted that:

- CCTV recordings, whether they contain *Personal Information* or not, will be retained by Council for a minimum of seven (7) days. CCTV recordings that have not been downloaded, will be automatically overwritten and the information consequently disposed of.
- Recordings obtained via a body worn camera or vehicle mounted camera will be held for no more than seven (7) days, unless footage specifically identifiable by location, time and content is retrieved and retained by an *Authorised Person* or *Authorised Individual* with the permission of the Chief Executive Officer (or the Chief Executive Officer's delegate).

---

[28] IPP2 and IPP3, Schedule 3 Information privacy principles, *Information Privacy Act 2009*.
[29] s29, Information Privacy Act 2009; definition of 'law enforcement agency', Schedule 5, *Information Privacy Act 2009*; s1(b), Schedule 1 Information privacy principles, *Information Privacy Act 2009*.
[30] s29, Information Privacy Act 2009; definition of 'law enforcement agency', Schedule 5, *Information Privacy Act 2009*; s1(b), Schedule 1 Information privacy principles, *Information Privacy Act 2009*.
[31] Schedule 3 Information privacy principles, *Information Privacy Act 2009*.
[32] IPP4, Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

- Any recordings or images downloaded from Council controlled cameras and retained in in Council's *EDRMS* will be disposed of in accordance with the General Retention and Disposal Schedule.[33]

Disclosure of Personal Information
Council will only disclose *Personal Information* obtained via Council controlled cameras in accordance with the purpose for which it was obtained, or in the following circumstances:

- to the Queensland Police Service for law enforcement services;
- when complying with requests to access records in accordance with the provisions of the *Right to Information Act 2009*, the *Information Privacy Act 2009* and by Court Order;
- where required or compelled to by law;
- in case of emergency or serious threat to the life, health, safety or welfare of an individual or to the public e.g. Council may provide CCTV footage to agencies other than the Queensland Police Services, limited to those agencies responding to or assisting with disaster management, such as the Queensland Fire and Rescue Service, Queensland Ambulance Service or the State Emergency Services; or
- a legislated exception applies[34].

A request to access CCTV recordings will need to be made in writing to Council, preferably via Council's CCTV Information Request Form (F563). The Director Corporate and Community Services will need to assess the approval and provide a written decision to refuse, or approve the request in whole or in part, if satisfied that:

- the written request provides sufficient and specific information about the recordings requested,
- there is sufficient evidence for a decision to be made about whether the disclosure is justified, and
- the disclosure will not be contrary to the *Information Privacy Act 2009*.

In the event of a privacy complaint, the onus will be on Council to demonstrate that disclosing the *Personal Information* acted in compliance with the privacy principles.

A record of the request, decision and any documents, images or recordings disclosed will be kept in Council's *EDRMS*.

4.2.4 Security and Monitoring
The proper management of *Confidential Information* and *Personal Information* will be monitored in accordance with the process outlined in both Clauses 4.1.6 and 4.4.5 of this policy.

4.2.5 Data Breach
Data Breach is any kind of unauthorised access, disclosure or loss of *Personal Information*. Examples of a potential *Data Breach* include, but are not limited to:

- opening an email and clicking on a link or attachment that may not be from the sender it purports to be from
- failing to use the BCC function on an email to a party external to Council
- sending an email containing personal information to the wrong person

[33] General Retention and Disposal Schedule, Queensland Government < General Retention and Disposal Schedule (GRDS) | For government | Queensland Government >.
[34] IPP10, Schedule 3 Information privacy principles, *Information Privacy Act 2009*; IPP11 (1)(e), Schedule 3 Information privacy principles, *Information Privacy Act 2009*.

- unauthorised access to personal information by an employee (outside the scope of their employment)
- losing a thumb drive on public transport
- something sensitive dropping out of your bag in a public place
- failing to lock your Council issued computer when it is unattended
- leaving hard copy documents containing *Personal Information* unattended or accessible to unauthorised persons
- having Council issued *ICT* equipment (e.g. computers, phones, etc.) misplaced or stolen.

Possible consequences of a data breach include the following examples of harm provided by the Office of the Australian Information Commissioner:

- *financial fraud, including unauthorised credit card transactions or credit fraud*
- *identity theft causing financial loss or emotional and psychological harm*
- *family violence*
- *physical harm or intimidation.*[35]

Council is committed to preventing, detecting and responding to data breaches quickly and effectively. Council uses the following measures to minimise the likelihood of an information security or data breach:

- technical controls (minimising access and modification capabilities, *Least Privilege*, *Need to Know*, etc.)
- administrative controls (policies, procedures, contractual obligations retention and destruction schedules)
- physical controls (locked doors, swipe card access to Council buildings, etc)
- *Staff* training
- creating a culture of reporting.

When contracting with parties external to Council, and those parties will have access to or manage Council data, Council must ensure that there are conditions within the contract with the chosen vendor that indicate:

- that the vendor is bound to comply with Queensland legislation relating to privacy
- that Council has the right to check that the vendor is doing what they say they will with the data, e.g. fulfilling their contractual obligations, legislative obligations, etc.

Council is committed to empowering *Staff* to report breaches, including those they:

- are directly involved with, and
- may see as a bystander.

4.2.6 Data Breach Response Plan

Council's C015 – P03 Data Breach Response Plan is designed to help Council limit the consequences of a breach, including the risk of harm to individuals whose privacy has been affected. **It should be noted that Council will not make ransom payments.**

Should a *Staff* member know, suspect or become aware of a potential *Data Breach*, the *Staff* member must report it to a *Privacy Officer* immediately, and depending on the nature of the potential breach, the ICT Team. The *Staff* member will need to complete a C/015 – P03 – 01

[35] Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1998 (Cth) – July 2019,* page 8, Data breach preparation and response (oaic.gov.au).

Data Breach form for the *Privacy Officer/s* to action and ensure the form is registered to Council's *EDRMS*.

4.2.7 Cyber Incident Response Plan (CIRP)

Council's ICT – OP04 Cyber Incident Response Plan supports an effective and coordinated response to cyber incidents, including post-incident reviews to improve future response.

A *Cyber Security Event* occurs when something is detected and requires further analysis to determine if a *Cyber Security Incident* has occurred. Should it be determined that the *Cyber Security Event* should be classified as a *Cyber Security Incident*, Council's Cyber Incident Response Plan will be enacted.

4.3 COUNCIL WEBSITES AND SOCIAL MEDIA ACCOUNTS

The ICT Team will be responsible for the production and maintenance of Council's *Corporate Website.* The production and maintenance of all other *Non-Corporate Websites* sites are the responsibility of the relevant section's Manager or Team Leader.

Requests for additional *Non-Corporate Websites* require Council approval. Approval for new pages on existing *Corporate Websites* or *Non-Corporate Web*sites are to be approved by the relevant Director.

The Communications Manager will be responsible for the production, maintenance and registration of posts and comments on Council's *Corporate Social Media* accounts. The production, maintenance and registration of all other Council social media accounts are the responsibility of the relevant Manager.

4.3.1 Website Content

Each Director is responsible for the accuracy and maintenance of all content relevant to their Department and as such, are required to sign the Website Information Request Form prior to any proposed changes being made. *Staff* are responsible for the provision and maintenance of content.

All content to be uploaded to Council's websites must comply with Council's C021 Style Guide Policy and Brand Identity Guidelines. Should further clarification be required, *Staff* should consult the Communications Manager.

The *Staff* member completing the Website Information Request Form is responsible for ensuring the information is reviewed and updated.

4.3.2 Promotions

Council's *Corporate Website* allows for promotion of key events on the home page. These specific promotional areas (located in the middle of Council's homepage) will be updated weekly and will remain on Council's webpage in that specific spot for one (1) week.

Council's Communications Manager will determine what content fills these spots each week. Priority will be given to upcoming events, promotions, surveys or events where RSVP dates or deadlines apply.

4.3.3 Exceptions

Documents that are regularly (daily, weekly or fortnightly) uploaded onto Council's *Corporate Website* (i.e. agendas, minutes and media releases) do not require a Website Information Request Form to be filled out. These documents are directly emailed to the ICT Team for uploading to the *Corporate Website* at the same time they are distributed to the public.

Blanket expiry dates will apply to specified content on Council's *Corporate Website* as follows:

- media releases are removed six (6) months from date of release
- agendas are removed and replaced with current Council minutes twice per month
- minutes are removed two (2) years from date of publication
- images uploaded to Council's gallery will be removed 12 months from date of publication
- budget material removed and replaced with current budget information annually.

4.3.4 Auditing of Website Content

Each Council department will appoint one (1) person with the responsibility of:

- reviewing website content for their department every six (6) months
- liaising with the relevant person / people to amend or remove content, as required.

The Communications Manager will regularly check the Website Content Management diary to ensure information on Council's websites is current. Should an *Elected Member* or *Staff* member notice content that requires amendment, the Communications Manager should be notified.

4.4 PROTECTION OF CORPORATE INFORMATION AND CYBERSECURITY

Somerset Regional Council recognises that a significant level of information risk exists due to a growing reliance on digital and cloud-based platforms, as well as the introduction of Artificial Intelligence (AI) based software. Council is committed to maintaining a focus on information security through a variety of policy and technical controls. Risks and the effectiveness of controls intended to manage those risks are periodically reviewed based on the following objectives:

- Confidentiality – ensuring that information is only accessed by an *Authorised Individual* and for authorised purposes.
- Integrity – ensuring the authenticity, accuracy and consistency of information.
- Availability – ensuring that an *Authorised Individual* is able to access information required to perform their appointed role.

Moratorium on new software

No new *Systems* (including software) that would be used for the capture and recording of *Personal Information* is to be acquired (including purchased, leased or acquired as software as a service) until the completion of agreed actions in sections 3.1, 3.3 and 3.5 in the internal audit report "Information Security Control Environment" of February 2023 (Document ID 1581771).

The following measures must be adhered to in order to minimise risk to Council's *Corporate Information.*

4.4.1 Data Classification Framework

In order to implement mitigation strategies to protect Council's *Corporate Information*, Council needs to identify its assets and the level of protection required from various threats. The Chief Executive Officer is responsible for establishing and maintaining Council's Data Classification Framework, data hierarchy and specifying a *Data Owner* (including responsible and accountable *Staff*).

The below table documents the Chief Executive Officer's data hierarchy, with Financial data, particularly payroll and accounts payable, being identified as Council's most critical data.

Data Category	Responsible (DATA OWNER)	Accountable	Classification
Financial *including payroll/ accounts payable/ financial/ rating system and ephemeral data* on data drive*	DFIN	DFIN	Most critical
Corporate records *including EDRMS and physical records*	DCORP	DCORP	
Spatial *including ephemeral data* on data drive but excluding Planning Scheme*	DOPER	DOPER	
Planning and Development *including ephemeral data* on data drive and Planning Scheme spatial data*	DPAD	DPAD	
Human Resources *including ephemeral data* on data drive*	DHRCS	DHRCS	
Executive *including ephemeral data* on data drive*	CEO	CEO	
Operations *Including ephemeral data* on data drive, CAD, flood studies, LIDAR, Reflect*	DOPER	DOPER	
Tourism and marketing *including ephemeral data* on data drive*	DCORP	DCORP	

Further information relating to Council's Data Classification Framework can be found in C015 – P01 ICT Management and Security Procedure.

4.4.2 Data Backups and Recovery

Ensuring reliable information backups is crucial for protection against data loss and business continuity. It also contributes to overall business resilience.

Backup controls are implemented to ensure:

- recovery from loss of data or systems,
- access to backup copies of information,
- data in Council's *Systems* is maintained and tested in a manner reflective of its classification in the Data Classification Framework.

Data backup and restoration processes mitigate the security risk of losing access to *Systems* or important data as part of a ransomware or other destructive form of attack. Regularly testing restoration backups ensure the integrity of the backup is not compromised and can be relied upon as part of a disaster recovery exercise.

Further instructions relating to data backup and recovery can be found in C/015 – P01 ICT Management and Security Procedure, ICT – OP01 Business Continuity Plan and ICT – OP06 ICT Team Manual.

4.4.3 Physical Security Controls

Access to Council's corporate facilities is restricted to *Authorised Individuals*, requiring a signed-out key or fob assigned to a specific *Authorised Individual*. Fob access is monitored, and higher security areas are restricted to *Authorised Individuals* granted *Privileged Access*.

Corporate facilities are also secured by monitored alarm systems when unattended.

Visitors to corporate facilities, including contractors, are required to:

- identify themselves before entry,
- note details in the entry log (where practical), and
- be accompanied by an *Authorised Individual.*

Physical access to Council's *Corporate Information Systems* or *Systems* are restricted by various physical and technical controls, including, but not limited to:

- A 10 minute screen password protected auto lock on all Council computers, tablets and phones (by Council's ICT Team if the device is issued by / controlled by ICT on Council's behalf) or by the *Authorised Individual* if the device is controlled by the *Authorised Individual* (for example, a device to which Council's C040 Opt-In Bring Your Own Device policy applies).
- All *Authorised Individuals* manually locking their computer screens when or if the screen is out of sight of the *Authorised Individual.* Failure to do so may result in *Disciplinary Action*.
- All *Staff* who keep or use paper based documents, or information in any other format readable by unauthorised individuals (e.g. removable storage media), containing:

    - *Confidential Information*,
    - *Personal Information*, or
    - *Corporate Information* that is not publicly available,

    will be required to secure the information from unauthorised access, when it is out of sight of the *Authorised Individual*, and especially outside normal business hours. Lockable cabinets and drawers are available to *Authorised Individuals* for security purposes. For clarity, it is a required that all *Staff* have a desk clear of sensitive information. Failure to do so may result in *Disciplinary Action*.

    Contractual arrangements with cleaners and other suppliers attending corporate facilities outside normal business hours will contain relevant privacy and probity requirements.

4.4.4 Change Management, Approved Access and Account Management

Change management mitigates risks, promotes smooth transition to new technologies and fosters a positive and adaptive culture in evolving technological landscapes. Changes to technologies used in the workplace environment, especially when transferring software from development to the operational environment, may impact on the integrity and availability of Council *Systems.*

Change Management

- The only authorised *Systems* for undertaking Council business are contained within the ICT Service Catalogue. Proposals or requests for new *Systems*, or major changes to existing *Systems*, are to be submitted to the Information Services Manager, in writing, with the following information:

- reason for purchasing, proposed use, desired outcome;
- options available from multiple service providers, if possible;
- initial cost, hardware costs, servicing costs, technical support costs, possible upgrade costs;
- compatibility with existing and planned *Systems*
- multi-factor authentication and other security capabilities;
- details of data intended to be held in the *System* for data breach notification and response purposes;
- details from the provider on data backups, ownership, retention and contract termination conditions, and, if personal or confidential data is to be held, details from the provider on data sovereignty, privacy and security;
- vendor business continuity plan.

The Information Services Manager will assess the proposal and provide feedback before submitting to the Chief Executive Officer for a final decision. Should the Chief Executive Officer approve the purchase and implementation of a new *System*, it will be added to the ICT Service Catalogue, a *Software Liaison* appointed and the Data Breach Response Plan and Cyber Incident Response Plan updated (if required).

Further instructions relating to implementation of approved new *Systems* or major changes to existing *Systems* is contained in C015 – P01 ICT Management and Security Procedure.

Approved Access

- A completed Employee Permissions Form (F841) is required prior to any new access or permissions, or changes to access or permissions, being implemented for each *Authorised Individual*. The *Authorised Individual* is to be positively identified prior to access being granted.

- Access is based on the security principles of *Least Privilege* and *Need to Know*, with *Group Membership* used to define access where possible. Attempting unauthorised access, allowing unauthorised access, or the unauthorised distribution of *Corporate Information* will result in *Disciplinary Action*.

- *Privileged Access* must be limited to *Authorised Individuals* responsible for administering a *System* and must not be used to perform tasks that can be undertaken at a non-privileged level of access.

- Where feasible, technical controls will generate alerts for new access or permissions, or changed access or permissions.

- Network user and computer accounts are to be removed when no longer required and reviewed at least every two (2) months to identify any orphaned accounts, based on recent usage.

- Physical access is to be removed if no longer required.

- Shared or anonymous access is not permitted to any *System*. Library circulation computers are the only exception due to workflow requirements, and these must only have access to internal library emails and the library management system.

- *Authorised Individuals* have a responsibility to manage and protect access to their *Systems,* credentials and contact phone numbers. This includes:

  - securing *Systems* when not in use or unattended to prevent unauthorised use;
  - using their own user name / login / passwords, etc;

- sending emails using their own email account;
- providing the publicly available Council phone numbers to people external to the organisation, rather than a direct extension line or mobile phone number (where possible);
- keeping Council issued equipment secure and in good working order,
- protecting *Systems* from intentional or negligent damage, be it:

    - physical damage,
    - damage caused by propagation of computer viruses or other damaging software,
    - downloading, installing, using or modifying software or hardware on a *System* without approval from the ICT Team,
    - connecting a device (i.e. USB, external storage devices, mobile phones, etc.) not owned by Somerset Regional Council and approved by ICT, without the express written approval of the Chief Executive Officer,
    - or by any other means.

- *Systems* should only be used for legitimate Council business purposes. Failure to do so will result in *Disciplinary Action*. *Systems* will be logged and monitored for potential inappropriate and / or unauthorised access,use, habits or behaviours. For example:

    - Email addresses issued to *Authorised Individuals* are provided for work purposes and should not be used for personal matters.
    - Council's phone system may monitor and record phone calls at any time.
    - *Elected Members*, *Staff* and visitors in the vicinity of Council facilities are likely to have their image and voice captured on Council's CCTV system, which may be monitored and retained in accordance with this policy.

  Council gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed whilst using Council *Systems* for personal purposes, or when in the vicinity of Council's CCTV system.

- Remote access to Council *Systems* is by exception and will require approval from the *Authorised Individual*'s Director and the Chief Executive Officer. Access to *Corporate Information* will be provided only via Council supplied assets except in the following circumstances:

    - where Council policy specifically permits;
    - vendor access is approved to specific *Systems* for support purposes;
    - at the discretion of the Chief Executive Officer in emergency circumstances such as a defined disaster. Should this scenario apply, the remote access details and credentials are configured by the ICT Team and are not to be provided to end users.

4.4.5 Security and Monitoring

All *Elected Members*, *Staff* and *Authorised Individuals* are responsible for the security of *Corporate Information* and *Systems*. Failure to do so may result in financial losses, reputational damage, operational disruption, legal consequences and a range of negative impacts to overall business resilience and sustainability.

All *Systems* and network traffic may be monitored at any time. *Elected Members*, *Staff* and visitors in the vicinity of Council facilities are likely to have their image and voice captured on Council's CCTV system, which may be monitored and retained in accordance with this policy.

Council may undertake surveillance of Council's *Systems*, for any *Authorised Individual*, at any time, without providing notice to the *Authorised Individual.* This includes the review of images and sounds captured on Council's CCTV systems of *Elected Members* and *Staff.*

Surveillance may also occur in relation to:

- storage volumes
- internet sites (every internet site visited is recorded, including the time of access, volume downloaded and the duration of access);
- suspected malicious code or viruses;
- emails (the content of all emails received, sent and stored including emails deleted from the Inbox);
- any storage location, whether computer network or cloud
- workplace actions and behaviour
- checking facts or a timeline.

Council has met all costs associated with the provision of *Systems* and access to the Internet, including access line rental. Any additional costs incurred due to personal use of the Internet or Council network must be met by the person enabling such costs to be incurred, including but not limited to, excess bandwidth charges, printing costs, specific charges to utilise a particular website, etc. *Disciplinary Action* may also be taken.

Council retains logs, backups and archives of all *System* activities and retains CCTV footage in accordance with this policy. The contents therein are the property of Council and may be used for various purposes, including but not limited to, auditing, complying with requests to access records (in accordance with the provisions of the *Right to Information Act 2009*, the *Information Privacy Act 2009*, or by Court Order), undertaking workplace investigations, ensuring compliance with Council policies, etc.

The ICT Team reserves the right to prevent (or cause to be prevented) the delivery of an email or access to an internet website, if such email or access poses a potential risk to *Corporate Information* or *Systems.*

The Information Services Team will undertake quarterly testing of *Authorised Individual*'s compliance with this policy. This may take the form of sending emails that resemble infected emails, auditing email use and *Public Record* registration, or undertaking any other relevant means of testing the security and accuracy of Council's *Corporate Information* and *Systems*. This testing may be conducted for all *Authorised Individuals* or selected *Authorised Individuals* (including by random selection).

Test results will be recorded on employee personnel files in Council's *EDRMS*. The outcome of testing will help inform Council's cybersecurity and record keeping strategies, including whether additional training is required, and the main sources / areas of risk. Unsatisfactory test results to identified risk, demonstrated on a repeat basis, will result in *Disciplinary Action* and additional controls being implemented for relevant *Systems*. It should be noted that:

- *Elected Members* and *Staff* that fail phishing tests will be advised of the failure within 30 days, and will be required to undertake and pass Information Management and Security refresher training, and
- *Disciplinary Action* will be taken for all *Staff* who fail phishing tests more than once in a three year period.

The Information Services Team will report to the relevant Director and Chief Executive Officer when the actions of an *Elected Member*, *Staff* member or *Authorised Individual* have breached, or are suspected to have breached, this policy and/or any other Council policies or procedures.

If the Information Services Team have concerns about staff capabilities at any time, especially post-test, they must raise this with the relevant Director and/or the Chief Executive Officer, in writing.

4.4.6 Password Controls

- *Systems* are to be secured by a minimum of unique identifier and authenticator, and multi-factor authentication where possible.

- Passwords are to have sufficient factors, length and complexity to delay an attacker's attempt in systematically checking all possible passwords until the correct one is discovered (dictionary attack).

- Passwords are not to be shared.

- Vendor supplied and/or default passwords are not to be used on any *System*.

- Password management standards will be implemented as a technical control where possible on all *Systems*, and by policy control and awareness campaigns where technical controls are not feasible.

- *Privileged Access* passwords for *Systems* must be stored in a secured location that provides adequate access controls, role-based delegation and capacity for auditing.

- **EFFECTIVE 30 JUNE 2024, unless authorised by the Chief Executive Officer in writing for any nominated *System*:**

    - **Multi-factor authentication will be installed in all *Systems***
    - **passwords in all *Systems* will be forced to be changed every six (6) months**
    - **the password standard will be at least 14 characters**
    - **the previous five (5) passwords of the user will be unable to be used.**

4.4.7 Cloud Services

Cloud Services can involve shared responsibility for information security between the cloud service provider and Council as the cloud service customer. Responsibilities for both the cloud service provider and Council must be defined and implemented appropriately in order to manage information security risks[36].

Relevant considerations when making this assessment are outlined Clause 4.4.4 'Change Management' of this policy and in Council's C015 – P01 ICT Management and Security Procedure.

Elected Members and *Staff* are not permitted to use work credentials, such as Council issued email address or phone number, for personal matters as it increases the risk of the Council issued email address or phone number being captured in a *Data Breach*. For example, using a work email address to log in to your personal accounts for myGov, Medibank, electricity provider, etc. means your Council issued contact details may be compromised and increase the risk to Council of a *Data Breach* occurring.

4.4.8 Artificial Intelligence (AI)

Generative artificial intelligence (AI) is a type of AI used to create new content, including text, audio, images and videos in response to prompts input by a person. Some generative AI

[36] Note s33 of the *Information Privacy Act 2009* relating to the transfer of an individual's personal information to an entity outside of Australia.

systems are unsecured (e.g. Chat GPT) and others claim to be secured (e.g. Microsoft 365 Copilot).

The use of generative AI systems presents a significant risk to Council's *Corporate Information*, *Confidential Information* and *Personal Information*. Council's Chief Executive Officer may permit specified *Authorised Officers* to use a specific generative AI system within specified parameters. These requirements will be specified in C015 – P01 ICT Management and Security Procedure.

Authorised Officers must take steps to verify AI generated information is accurate and unbiassed, as the quality of the AI generated material may be compromised if incorrect or biased information is inputted and ingested by the program being used i.e. there is capacity to 'poison' the AI generated material.

4.4.9 Review Process

A review of Council's information security at a practical level will be requested as part of internal audit processes at least every three (3) years.

4.5 TRAINING AND SECURITY AWARENESS

Information Management and Security training is required to be undertaken by all *Elected Members* and *Staff.* This training will reinforce that breaches of this policy, or associated policies and procedures, may result in *Disciplinary Action*.

Training will be delivered upon commencement of employment, with annual refresher training to be undertaken. Additional training and awareness campaigns may be tailored to specific individuals, groups or teams if auditing or testing indicates that it is required in order to adequately manage risk to Council's *Corporate Information* and *Systems*.

Software Liaisons will be required to undertake additional training on Right to Information and Information Privacy applications annually.

Supervisors and *Software Liaisons* are responsible for providing additional training, when required. Should the Information Management and Security training provided not include guidance for a specific problem regularly identified during the auditing / testing process, *Software Liaisons* will liaise with the Information Services Team to amend the Information Management and Security training, where necessary.

Supervisors of *Staff* are responsible for:

- ensuring *Staff* are performing to a satisfactory standard,
- enabling *Staff* to attend any training necessary for the development and / or maintenance of skills applicable to their position with Council, and
- managing performance and taking *Disciplinary Action* where required, if Council's legislated information management and security obligations, as outlined in this policy and associated procedures, are not being met.

Security awareness will be promoted by including:

- an article about cyber security in every staff newsletter issued with fortnightly pay slips, and
- a standing agenda item on each quarterly Team Somerset Management Committee (TSMC) meeting for 'ICT Systems and Cyber Security'.

5. DATE OF RESOLUTION

This policy was endorsed by the Chief Executive Officer and adopted by the Somerset Regional Council at the Ordinary Meeting of 27 November 2024, with an effective date of 5 December 2024.

Signed:  Date: 27 November 2024