POLICY NO	**CP/ICT-3260**	
POLICY	**Information Management and ICT Acceptable Use**	
RESPONSIBLE DIRECTORATE	Corporate Services	
RESPONSIBLE OFFICER	Manager ICT	
COUNCIL ADOPTION	Date: 15/12/2015	Resolution No: 11208
REVIEWED/MODIFIED	Date:	Resolution No:
	Date:	Resolution No:
REVIEW DUE	Date: ~~December 2017~~ April 2019	
LEGISLATION	*Local Government Act 1995* *Privacy Act 1988* *State Records Act 2000 (WA)* *Freedom of Information Act 1992 (WA)* *Broadcasting Services Act 1992* *Broadcasting Services Amendment (Online Services) Act 1999* *Electronic Transactions Act 1999* *Copyright Act 1968*	
RELATED POLICIES	~~CP/ICT-3261 Mobile Device Management (new Policy currently being drafted)~~ ~~Code of Conduct for Council Members, Committee Members and Employees~~ CP/GOV-3102 Media & Corporate Communications ~~Personal Use of Social Media (new Policy currently being drafted)~~	
RELATED ORGANISATIONAL DIRECTIVES	~~OD/ICT-4260 Information Management and ICT Acceptable Use~~ ~~Information Statement (relevant to current year)~~ ~~Recordkeeping Plan 2012~~ Recordkeeping Plan 2017	

PURPOSE:

The purpose of this Policy is to demonstrate Council's commitment in upholding the legislative and administrative requirements in the use of the Shire of Wyndham East Kimberley's Information,

Communication, and Technology (ICT) resources and associated Information Management (IM) framework.

This Policy recognises the importance of maintaining effective controls over information security, operational guidelines, and records management procedures.

The concepts contained herein are necessary to mitigate data loss, Shire reputational damage, and facilitate productivity throughout the organisation whilst complying with requisite information management standards including State and Federal legislation.

DEFINITIONS:

Authorised Persons means a member of the Executive or members of the ICT department including delegated representatives.

Authorised User means any person, whether an employee, elected member, or contracted party, whom has been granted authorised access to the Shire's systems and services.

BYOD means Bring Your Own Device - the practice of granting users corporate network access in order to use their personal mobile devices for business purposes.

Corporate Knowledge represents any tangible or intangible file, record, or communication thread or intellectual property that holds value for the purposes of conducting business; whether particulars be related to past, present, or future.

Electronic Communications means email, instant messaging, and any other material sent electronically.

Email System means Shire provided Microsoft Outlook, Outlook Web Access, or any Shire email system that is synchronised to a PC or mobile device; whether the mobile device is provided by and remain the property of the Shire, or owned by an authorised user.

ICT means Information, Communications, and Technology.

Information System is any organised system for the collection, storage, and communication of information.

Malware is an abbreviation of 'malicious software' and means software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware, ransomware and trojans.

Misconduct means unacceptable or improper behaviour, especially by an employee or affiliated person. Refer to the adopted Code of Conduct for Council Members, Committee Members and Employees.

Network Access includes connectivity from any device to Shire managed ICT infrastructure connecting both local and remote network servers.

Personal Use means all use that is not specifically related to the Shire of Wyndham East Kimberley.

The Cloud or **Cloud Computing** describes off-site network services made available to local users over the internet. Examples are Hotmail, Google Docs, Dropbox, Doc Assembler, Docs on Tap etc.

A **Record** is defined as meaning "any record of information however recorded" and includes:

- anything on which there is writing or Braille;
- a map, plan, diagram, or graph;
- a drawing, pictorial or graphic work, or photograph;
- anything on which there are figures, marks, perforations, or symbols, having meaning for persons qualified to interpret them;
- anything from which images, sounds, or writings can be reproduced with or without the aid of anything else;
- anything on which information has been stored or recorded, either mechanically, magnetically, or electronically.

Records and Document Management means any system or service, whether hosted by the Shire or in the cloud that is responsible or related to the storage or filing of corporate data and knowledge. This is inclusive of records management systems or shared file storage.

A **Records Manager** is a user who administratively works with Shire-related correspondence or other forms of documentation or communication, and is obliged to file such appropriately in line with adopted records management policies and procedures.

Shire means the Shire of Wyndham East Kimberley.

POLICY STATEMENTS:

All users must be vigilant in their adherence to these procedures in order to mitigate a plethora of risks that may negatively affect the Shire due to abuse or resulting from misuse. These measures are paramount in ensuring the Shire's business continuity.

1. *Objectives*
   The Council's objectives in establishing this Policy are to:
   a. Ensure there is an understanding of the obligations of users that are provided privileged access to information systems operated by the Shire of Wyndham East Kimberley;

   b. Ensure there is an awareness of the ownership of any intellectual property that resides on Shire information systems;

c. Ensure best practice policies and procedures are followed in relation to the operation of all information systems;

d. Ensure compliance with the *State Records Act 2000* and associated records management practices and procedures of the Shire.

This Policy encompasses the following five (5) principles of information security:

1. *Confidentiality*
   Ensuring that information is only accessible to those with authorised access. For example, this could mean using a strong password on your computer or mobile device, shredding sensitive documents, and locking filing cabinets.
2. *Integrity*
   Safeguarding the accuracy and completeness of information and processing methods.
3. *Availability*
   Ensuring that users have access to information when they require it, ~~ie.~~i.e. ensuring that no person or event is able to block legitimate or timely access to information.
4. *Compliance*
   Ensuring that the Shire meets all legislative obligations.
5. *Responsibility*
   Ensuring that appropriate controls are in place so that users have access to accurate, relevant and timely information, but that users of the Shire's ICT resources do not adversely affect other users or other systems.

All Shire records, files, and communications are considered a corporate asset, regardless of physical format, storage location, or date created and are essential to the business of the Shire.

All records will be registered in the Shire's corporate Records Management System inclusive of content and context. These records must be complete and accurate.

The Council is committed to developing and implementing information management practices which support the Shire's business and legislative requirements.

Ownership and proprietary interest of records and information created or received during the course of business is vested in the Shire.

The Shire will endeavour to retain and dispose of records and information in accordance with the retention and disposal schedules approved by the State Records Commission.

The Council is committed to capturing and preserving records and information of significant historical or cultural value to the Shire and the State.

2. *Acceptable Use*

The use of Shire ICT systems and content for illegal, offensive, or other inappropriate activities, is prohibited.

This includes but is not limited to:

- Interfering with the intended use of resources. Such activities may include the downloading very large amounts of data affecting the performance of internet bandwidth for all other users;
- Seeking to or gaining unauthorised access to any resource;
- Using or knowingly allowing another to use any system to defraud or to obtain money, property, services, or other things of value by false representations;
- Breaching the privacy of individuals without authorisation;
- Conducting a business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group or list members to use goods or services;
- Publishing information which violates or infringes upon the rights of any other person or group;
- Online gambling activities or political campaigning;
- Engaging in the use of social media tools for personal use during business hours; or
- Misrepresentation of yourself or the Shire of Wyndham East Kimberley.

3. *User Accounts*

Effective access controls and reporting require that all users and their actions be uniquely identified.

All network user-id's will be password protected. Passwords must be kept secret and not shared. Users are accountable for all activity conducted under their allocated user account(s).

Generic and/or shared network user-ids may also be necessary in specific situations. Creation and use of all such network user-ids must be approved by the ICT Manager.

You should observe the following with respect to your network user-id and password:

- Never divulge your password to another person, including system administrators, support staff, family and/or friends;
- Never write your password down in a conspicuous location;
- Take care that you are not being watched when you type it in;
- Change it immediately if you suspect that it has been compromised;
- Never allow another person to operate a computer session signed on with your network user-id and password without your supervision;

- You must never attempt to sign-on as another person, or use a session signed-on with another person's network user-id and password; and
- Your network user-id will be locked after 5 invalid login attempts to mitigate malicious access. You must contact the ICT Department to unlock the account.

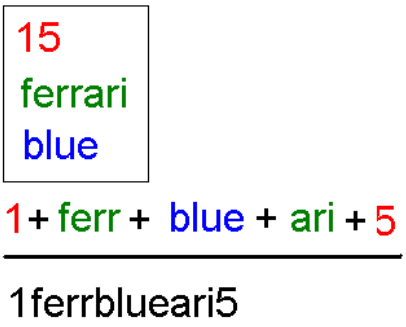
4. *Password Management*

Passwords are a common way to verify an identity. It is important that the password for your network user-id cannot be easily guessed.

You should observe the following with respect to your network user-id:

- Your password must have a minimum length of 7 characters;
- Passwords are case sensitive and subject to the following syntax rules:
  - Must consist of at least 1 numeric and 1 alpha character;
  - Must consist of at least 1 upper case and 1 lowercase letter;
  - Must not contain your name;
  - Your password will expire after 42 days;
  - You cannot reuse any of your last 24 passwords; and
  - Your password must not be a common word.

eg.



5. *Access Control*

Access to either the Shire's local or cloud based resources requires:

- A unique-id and password for ICT-based resources; and
- A business need to justify the access.

If you require access to any resource to perform your duties, log an appropriate ICT Helpdesk request noting if access is required / no longer required.

6. *Internet Use*

The Internet is a shared resource; and as such users must be considerate of others. Using the Internet in a manner that may cause offence or bring the Shire into disrepute is prohibited and may result in disciplinary proceedings.

Offensive material includes but is not limited to:

- Obscene or harassing language or images;
- Negative racial, ethnic, sexual, erotic or gender specific comments or images; and
- Other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, physical features, nationality or age.

The Shire permits and encourages its user base to access and use the Internet to carry out their duties, to contribute to the achievement of Shire business objectives and for staff development.

The ICT department will log all Internet activity. The Shire has the right to implement systems to automatically block access to certain sites that are considered to be either inappropriate or are being abused.

- You must not deny nor disrupt access to resources required by other staff in the performance of their duties. Such activity may include but is not limited to streaming media, excessive downloads, excessive non-business use and/or inappropriate sites;
- You must take all reasonable care when downloading, accessing or executing files on or from the Internet services. The consequences of introducing viruses or any other harmful software through the Internet environment may be serious and of great expense to the organisation;
- The ICT department should be contacted immediately if there is suspicion that a file, communication or information may contain a virus;
- You should be particularly careful of the potential for disclosing information on the Internet. The capture of information containing workstation details, browser settings, network and personal information is a significant risk on the Internet and contributes to network compromise and ‘phishing’ (tricks used to fool the user into surrendering private information that will be used for identity theft);
- You should not reuse an existing network user-id or password associated with the Shire on any public web sites. Since public web sites are outside the control of the Shire, there can be no assumption as to the security of the site. Using an important network user-id or password on such a site must be avoided;
- All software products must be authorised and licensed before being installed on any equipment; and

- You are reminded that copyright restrictions often apply to all Internet files including web page content, images and documents.

7. *Email*

   Email is an important business tool but is also subject to misuse. The organisation is committed to the appropriate use of this tool and expects all users to comply with acceptable usage directives.

   It is important to note that all email messages that are created, sent or received using the email service remain property of the Shire.

   - The Shire email system is to be used explicitly for the conduct of Shire related business. ~~ie.~~i.e. no use for personal communications is permitted.
   - You should not forward unsolicited email (spam) or items such as chain letters.
   - Emails are business records and should be filed into the records management system in the same way as any other business record and deleted from your Inbox. Any filing questions are to be referred to the records department.
   - Elected Members are to send a copy of pertinent Council-related email records, as defined by the State Records Act 2000, to records@swek.wa.gov.au where they will be registered appropriately.
   - Consider that emails are not necessarily delivered or read by the recipient immediately, so other forms of communication should be considered where the matter is urgent.
   - You should take reasonable care when opening attachments received with emails. If there is a suspicion that a file may be infected by a virus, you should contact the ICT department immediately.
   - Judgement should be used when forwarding emails that you have received to ensure you are not breaching the confidence of the sender.
   - Emails should be drafted in ~~a professional~~a professional manner. Adhere to acceptable standards of email etiquette; i.e. ~~All~~all capitals indicates 'yelling'. Address your recipient by name. i.e., Hi xxxx.
   - Email~~l~~ messages must not contain content considered to be offensive. If you receive material that you believe may be offensive you should respond to the sender professionally conveying your objection.
   - You should always use subject headings to help identify relevance of content for recipients.
   - Email should not be considered a file transfer tool. Consider use of accepted file transfer tools such as 'Dropbox' if sending large files to external bodies.

- A size quota may apply to your email account. Size violations will result in the inability to send email, until your inbox, sent items and subfolders, are reduced.

8. *Disclaimer*

The following disclaimer should be appended to all email sent from an officer or elected member in regard to the corporate email system:

The information contained in this email, including any attachments, may be confidential and / or contain legally privileged information. If you are not the intended recipient any use, disclosure or dissemination of this email is unauthorised. If you have received this email in error, please delete all copies, including any attachments and alert the sender. Virus scanning is the responsibility of the recipient.

Please consider the environment before printing this e-mail

---

9. *Shire's Email Addresses*

The Shire's primary public e-mail address is mail@swek.wa.gov.au. Emails to this address will be received by the Records Department who will register and distribute the email to the appropriate officer. Other mailboxes have been set up for specific purposes with the associated departments responsibly monitoring and processing the email received.

10. *Malicious Software*

Malicious software is a term used to describe programs that can maliciously attack and affect computer files and cause some unwanted actions whenever those files are used.

Viruses and Malware are examples of this.

The most common way for malicious software to be introduced to a system is via a file accessed from an external source, such as from a memory stick, e-mail attachment or by downloading a file from the Internet.

The aim of anti-virus software is to detect malicious software before it is introduced, and to identify and delete files already infected. However, new viruses are continually being developed and, although the virus protection software is regularly updated to keep pace with those developments, it is unrealistic to expect that anti-virus software can provide complete protection.

It is therefore important for all users to be careful that they do not introduce malicious software, and to be diligent in detecting unusual events and reporting them immediately to the ICT department.

- If you encounter a message indicating that a software virus has been detected but not cleaned you must advise the ICT department who will act to prevent any further distribution of the virus;
- Do not install browser plug-ins such as toolbar add-ins;
- Do not open any files attached to an email message from an unknown, suspicious or untrustworthy source;
- Do not open any files attached to an email message if the subject line is questionable or unexpected;
- If you receive an untrusted attachment, delete the file;
- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited and intrusive;
- You must not download files from suspicious web sites.

11. Computer Software and Licensing

Software that does not have a valid licensing agreement is not to be used on any Shire maintained equipment.

All software must be used in accordance with specified license or copyright terms and conditions.

Proprietary software licensed for use must only be loaded onto owned equipment. Copies must not be taken for use on other equipment, including privately owned equipment, unless explicitly permitted by the licensing agreement and /or authorised by the ICT Manager.

The download and installation of software to Shire owned equipment is only to be performed by the ICT department.

- You must comply with all formal licensing requirements with regards to all software;
- You must inform the ICT department of any software that you no longer require, so that it can be removed in a timely manner and reallocated if applicable;
- You must not install or use any unauthorised software designed to compromise or bypass any security controls. Use of such software is strictly prohibited and will be considered a significant breach.

12. Mobile Devices

Due to the portable nature of notebook computers and other mobile devices, there is a requirement to maintain physical and data security.

- You must take special care to ensure that the Shire's information is not compromised through use of mobile devices in a public place. You should attempt to ensure that

screens displaying sensitive or critical information cannot be seen by unauthorised persons;

- Never leave notebook computers or other mobile devices unattended in a public place, or in an unlocked house, or office. Where possible, they should be physically locked away.
- Do not modify settings for password validation on mobile equipment. If authentication (identity verification) is enabled, do not disable it.
- Use Wifi where available to minimise telecommunications provider costs (3G/4G).

13. Physical Security and Protection

Physical and environmental issues affect all aspects of information security. These issues range from unauthorised physical access and exposure to environmental factors such as fire and flooding.

Physical security must be provided for all information regardless of the technology and including telecommunications equipment or facilities to ensure that associated assets are adequately protected against loss, damage or other risk.

- Ensure that office sites are appropriately physically secured;
- Never allow external parties to access Shire premises network access points or wireless network system;
- Shire property must be adequately maintained cared for;
- Supplied protective covers must not be removed;
- Do not leave sensitive electronic equipment in hot vehicles.

14. Remote Access and Remote Working

All remote access to Shire information assets must be approved by the ICT manager.

- Use of a remote access facility to access systems will only be granted if it is consistent with information security standards;
- You will be held accountable for all actions performed under your network user-id and password;
- To facilitate this, you must never leave a remote access session unattended, even if you are not currently signed-on to an application or other information system;
- Always disconnect a remote access session immediately after you have signed-off an application or other system;
- Never allow another person to operate a remote access session that you have established.

15. *BYOD*

The Shire supports the flexibility afforded by a Bring Your Own Device scheme.

If and when approved by the ICT Manager, a user's personal device may be used to connect to Shire email and other selected information systems.

~~Consult the Council's Policy *CP/ICT-3261 Mobile Device Management* (currently being drafted) for further information.~~

16. *Incident Response and Issue Resolution*

It is important that all suspicious events which involve Shire information assets are:

- Reported;
- Investigated;
- Responded to in a timely manner; and
- Evaluated for business impact.

Routine Help Desk requests can be logged via the Shire's helpdesk portal; whereby the ICT Department will attend to resolution as soon as possible.

Sending an email to itsupport@swek.wa.gov.au noting the nature of the issue will automatically create a helpdesk request and assign it to an ICT staff member to action. Your will receive a return confirmation email.

Any irregular or suspicious activity should be reported to the ICT department. Support detail should include:

- Any evidence of the issue;
- The scope of the threat, incident, or fault;
- Details of any systems affected;
- The exact text of error messages;
- Screenshots if applicable.

17. *Roles and Responsibilities*

The **ICT Manager** is responsible for:

- The provision and implementation of assets, supporting systems, applications and processes that give effect to this policy.
- The establishment and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms function effectively.

- Facilitating an appropriate user induction of ICT system usage.

All users are required to adhere to the Shires ICT directives and Code of Conduct.
In extenuating circumstances, exceptions to procedures require the approval of the ICT Manager.

Employees, Elected Members, and authorised users are to create and maintain records relating to the business activities they perform in a manner commensurate with legislation, policy, and directives, for the effective management of corporate knowledge.

Employees, Elected Members, and authorised users are to comply with this policy.

The **Chief Executive Officer** must ensure that a fit-for-purpose system is made available for the maintenance and management of records and information that is compliant with records management legislation and State guidelines and procedures.

The Executive, Managers, and Supervisors are responsible for fostering and supporting a culture that promotes good recordkeeping and information management practices, and ensuring that records management organisational directives and work instructions are known and adhered to. This includes ensuring that users are appropriately trained.

All users must access ICT resources in a manner that does not contravene the law. Use must be appropriate and authorised.

All users are records managers.

Shire ICT resources and data may be accessed or monitored by Authorised Persons at any time without notice to the user. This includes, but is not limited to, use of email systems and other electronic documents and records~~; however~~; however, Authorised Persons must have a valid reason for accessing or monitoring such.

18. *Potential Outcomes of a Breach of the Conditions of this Policy to the Shire*

~~Non conformance~~Non-conformance with the ideals and requirements contained herein may result in:

- Breach of the Shire network by malicious parties resulting in data loss &/or reputational damage;
- Widespread viral/malware infection leading to loss of productivity;
- Unauthorised internal access to confidential material;
- Breaches of privacy;
- Access to and/or display of discriminative or offensive material;
- Legal proceedings resulting from inappropriate online activity;
- Significant incurred internet or call costs.

19. *Consequences of Contravening the Policy*

- May result in disciplinary action in accordance with the Code of Conduct for Council Members, Committee Members and Employees;
- May constitute an offence or crime under relevant state or federal legislation, resulting in prosecution;
- If a violation is considered a criminal offence, the appropriate law enforcement agency will be informed;
- The Crime and Corruption Commission will be notified if misconduct is suspected to have occurred.

EXPLANATORY NOTES:

The Shire operates a comprehensive suite of complementary software and hardware systems that underpin its operational and strategic needs. Many complex ~~integrated *information*~~integrated information *systems* operate upon this technology platform, of which necessitate informed and compliant usage.

In accordance the *State Records Act 2000*, State Records Commission (SRC) Standard 1: Government Recordkeeping – requires that government organisations ensure that records are created, managed and maintained over time and disposed of in accordance with the general disposal schedule for local government records.

This Policy provides elected members, employees, and contracted representatives with an overview of their obligations under legislative and operational guidelines.

This Policy does not cover the use of social media or specific technological applications.

The Policy approach of the State Records Commission in monitoring the recordkeeping obligations in respect to Local Government elected members is:

> *"In relation to the recordkeeping requirements of local government elected members, records must be created and kept which properly and adequately record the performance of member functions arising from their participation in the decision making processes of Council and Committees of Council.*
>
> *This requirement should be met through the creation and retention of records of meetings of Council and Committees of Council of local government and other communications and transactions of elected members which constitute evidence affecting the accountability of the Council and the discharge of its business.*
>
> *Local governments must ensure that appropriate practices are established to facilitate the ease of capture and management of elected members' records up to and including the decision making processes of Council."*

RISK:

Risk: Inappropriate use of social media by Shire staff and Councillors.
Control: Social Media use policy and Staff Code of Conduct included in staff induction.

Risk: Inability to meet legislative requirements due to failure in record keeping procedures.
Control: Recordkeeping Plan.
State Records Act 2000.

Risk: Failure to comply with legislative requirements leading to damage of reputation and/or financial loss.
Control: Review policies and procedures (eg building, planning, health, childcare) in accordance with review schedule.

Risk: Loss of services due to ICT infrastructure failure.
Control: Server Data backed up nightly to tape.
Limited server room battery backup available.