BUNBURY HARVEY
REGIONAL COUNCIL
HARVESTING RESOURCES FROM YOUR WASTE

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Contents

POLICY STATEMENT

Bunbury Harvey Regional Council (BHRC) is committed to ensuring staff members have access to appropriate information and communication technology (ICT) infrastructure, tools, training and support which assists them to undertake their work efficiently and effectively.

OBJECTIVE

This policy aims to provide BHRC with guidance in managing the ICT infrastructure and tools provided to staff and clients, and to ensure staff use of these resources is secure and appropriate.

This policy is not intended to guide staff in administration and use of the website and other electronic systems.

INFORMATION AND COMMUNICATION TECHNOLOGY FRAMEWORK

DEFINITIONS

Information and communication technology (ICT)	An umbrella term describing technology systems and objects that enable users to access, store, transmit, exchange and manipulate information, including computers, networks, telecommunications (telephone lines and wireless signals), software, data storage, and audio-visual systems. **ICT assets or equipment:** • Electronic hardware items that include computers, tablets, printers, multi-functional copiers, VOIP hardware and software, mobile/smart phones, cameras, and data projectors. **ICT software:** Electronic software items that include programs, operative systems, data management systems and antivirus software programs. **ICT hardware or infrastructure:** • Interchangeable terms to describe ICT equipment along with cabling, modems, routers, phone lines and other equipment required for the operation of ICT assets. **ICT services:** • include internet services, web hosting, phone services, website development, and IT support. **ICT Officer:** • BHRC Officer / External IT Contractor responsible for managing ICT, including infrastructure and client and organisational systems. **ICT Systems:** • Sets of procedures or ways of doing things. ICT systems include protocols and policies put in place by an organisation or a third party relating to the use of or access to ICT hardware or software. **ICT System User:** • A person who is set up with access to the organisation's ICT systems. System users include all staff members but can also include anyone else who is explicitly authorised to use the organisation's ICT systems, including students, consultants, Elected members or volunteers.
Information management	Includes the creation, collection, storage, access, use and disposal of information assets.

Records	Records refer to all information created, sent and received in the course of carrying out the organisation's business.
Social media	Online tools or websites (e.g. Facebook, Twitter, YouTube, Instagram, etc.) that engage, create and share user-generated content, data and comments.
Software	Any form of computer program which provides a service to users, such as Microsoft Office Word (creates text-based reports), Internet Explorer (allows access to the internet), Outlook (email program), and so on.

PRINCIPLES

The following principles guides the BHRC's ICT policy and procedures:

a) Responsibilities for ICT management and administration are clearly defined.
b) ICT purchases are made for a valid reason, in an approved way and in alignment with the ICT Strategy.
c) ICT tools and systems are "fit for purpose" and responsive to changing environments and technologies.
d) All relevant laws are complied with, including laws relating to data protection, acceptable use of internet and email, software licensing, privacy, confidentiality, discrimination and harassment.
e) Staff are entitled to training and other support to assist them in using ICT Systems that are relevant to the work of the council.

OUTCOMES

The outcome of the policy is that BHRC has an ICT system which is:

- Secure
- Stable
- Efficient
- User-friendly

DELEGATIONS

Council	• Endorse and ensure compliance with the ICT policy. • Be familiar with the legislative requirements regarding communication, privacy and the collection, storage and use of personal information. • Understand the ethical standards with regard to communication, social media and the treatment of confidential information relating to the council's clients, staff and stakeholders.
CEO	• Ensure risk assessments are undertaken. • Monitor ICT budget and approve the expenditure of ICT equipment/services. • Ensure security processes regarding access of ICT systems. • Approve outstanding ICT expenditure.

	• Refer decisions to Council where expenditure is beyond general CEO delegation.
Staff	• Comply with the ICT policy. • Contribute to internal ICT strategies and activities. • Be familiar with the council's legislative requirements regarding communication, use of technology, privacy and the collection, storage and use of personal information. • Understand the council's ethical standards with regard to communication, social media and the treatment of confidential information relating to the council's clients, staff and stakeholders. • Ensure systems are in place across the organisation to communicate appropriately and to protect adequately the privacy of personal information of clients, staff members and stakeholders. • Monitor information and communications technology systems and procedures. • Ensure orientation of new staff members to the council's information and records management systems. • Facilitate alignment of ICT systems with other organisational programs, projects and activities. • Authorised staff members to make a request from the **approved IT Contractor,** for updating/purchase of new equipment in line with ICT strategy and plan. • Authorise access of new staff members or other people to the council's ICT systems. • Authorise the redirecting of emails from staff who no longer work with the council. • Responsible for reviewing ICT contract and budgets.
External IT Contractor	• Compliance with ICT policy. • Contribute to internal ICT strategies and activities. • Be familiar with the council's legislative requirements regarding communication, use of technology, privacy and the collection, storage and use of personal information. • Understand the council's ethical standards regarding communication, social media and the treatment of confidential information relating to council's clients, staff and stakeholders. • Maintain equipment and keep systems up to date. • Seek approval for ICT expenditure from CEO. • Ensure that requests from CEO for new/updated ICT equipment include notification as to whether a number of quotes are required. • Select suppliers and equipment and recommend to CEO. • Seek approval from the CEO for providing or removing access to ICT systems. • Provide staff and other authorised people with access to ICT systems.

	• In conjunction with BHRC Officer introduce new staff to ICT systems and provide support/training for ongoing use. • Recommend upgrades or service improvements in line with ICT strategy and/or based on changing environment. • Perform risk assessments, identify unacceptable risks to ICT, and consult with CEO on risk management strategy. • Make urgent ICT decisions to remedy a disaster, vulnerability or unacceptable risk to the organisation's security, reputation or business effectiveness.

POLICY IMPLEMENTATION

This policy is developed in consultation with BHRC employees and approved by council. All staff are responsible for understanding and adhering to this ICT Policy.

Specific monitoring and support activities undertaken include:

- ICT updates that are a standing agenda item in staff meetings
- This policy is to be part of relevant BHRC staff orientation and confidentiality processes
- This policy should be referenced in relevant council policies, procedures and other supporting documents to ensure that it is familiar to all relevant staff and is actively used.
- This policy will be reviewed in line with relevant legislative changes.
- Supervision of External IT Contractor.
- Report on ICT in the council's Annual Report and other relevant publications.

RISK MANAGEMENT

BHRC is committed to organisational risk management practices, systems and processes that ensure consistent, efficient assessment of risk in all planning, decision making and operational processes.

BHRC develops and implements information and communication technology systems informed by and complying with relevant legislation. This ensures these systems are effective as well as regularly monitored.

Other risk management actions include:

- All staff are made aware of this policy during the orientation process.
- Staff are provided with ongoing support and training to assist them to use ICT systems safely.
- As part of the council's Policy Review Schedule, this policy will be reviewed biennially unless circumstances require an earlier review and update.
- The need for improvements can be identified by council, management, staff member or client through feedback.
- ICT systems and plans are appropriately monitored and controlled by the allocated BHRC Administration Officer in conjunction with the authorised IT Contractor.

ICT STRATEGY

This section ensures that BHRC develops and implements a consistent ICT strategy to effectively manage internal information and communication technology systems, in order to enhance the council's operation and achieve its strategic goals.

Provides guidance on the plans, mechanisms and tools that BHRC adopts in order to prioritise and provide organisational strategies for resolving ICT needs and inform ICT decision making.

- Develops and implements a consistent ICT strategy to effectively manage internal information and communication technology systems, in order to enhance the council's operation and achieve its strategic goals;
- Provides guidance on the plans, mechanisms and tools that BHRC adopts in order to prioritise and provide organisational strategies for resolving ICT needs and inform ICT decision making;
- Establishes an ICT culture and a strategy that integrates ICT with the council's mission and values;
- Ensures that ICT complements and enhances the council's service to its clients;
- Provides a structure for the continuing development of digital proficiency;
- Enhances the role of ICT in fulfilling council's mission and improving its function;
- Builds awareness of the cultural and operational importance of the digital cultural.

PURCHASING OF ICT EQUIPMENT, SOFTWARE AND SERVICES

BHRC encourages the appropriate and timely acquisition of ICT equipment to support the council's operations, including research, programs, services and activities.

This section provides guidance to BHRC in purchasing ICT equipment, software and ICT services to suit the council's needs.

Council ensures that all ICT equipment, software and services are used and disposed of in an ethical and responsible manner and recognises the need to be consistent, cautious and thorough in the way that these tools support the council's operations.

This section ensures that:

- BHRC provides quality, reliable and up-to-date equipment and software to its employees in order to provide quality services.
- Council complies with both legislative requirements and ethical obligations in the purchase and use of equipment, licences and other ICT supportive services.
- All staff understand their responsibilities in relation to purchasing ICT equipment.

ICT TOOLS

As defined in Definitions of this policy, BHRC identifies different types of ICT tools; this includes:

- **ICT equipment:** electronic hardware items that includes computers, tablets, printers, multi-functional copiers, mobile/smart phones, cameras, and data projectors.
- **ICT software:** electronic software items that include programs, operative systems, data management systems and antivirus software programs.
- **ICT services:** include internet services, web hosting, phone services, website development, and IT support.

ICT PURCHASING OR ACQUISITION PRINCIPLES

The general principle underpinning this policy is that ICT purchases are made for a valid reason, in an approved way, and in alignment with the ICT Strategy.

BHRC is committed to purchasing the most cost-effective ICT goods and services primarily with regard to price, but also relating to quality, reliability, service, delivery and efficiency. This may mean, for example, that a slightly higher priced item or service might be chosen if it is from a supplier that has proven to be reliable in the past.

BHRC has a commitment to consider environmental and ethical manufacturing issues wherever possible.

ICT PURCHASING

Where the authorised IT Contractor in conjunction with the CEO determines that new ICT equipment, software or services are required as part of the maintenance of current ICT infrastructure, or to further the implementation of the council's ICT Strategy, the following procedures are utilised:

- The authorised IT Contractor sources the item, keeping in mind and adhering to the council's Purchasing Policy.
- The authorised IT Contractor collects relevant information about the item and the quote/s, and present these to the CEO for approval.
- Once approval is given, the authorised IT Contractor can place the order.
- The authorised IT Contractor can arrange to pay requesting the supplier for the goods supplied to be payable on account/invoice.
- When the item is delivered or the service commences, it is the responsibility of the authorised IT Contractor to ensure that it matches the order or the contract and that it is in perfect working order as per the product and technical specifications. Any disputes should be referred to the CEO. The Governance Assistant is responsible for entering the item into the asset register.
- Once the invoice has been received, the authorised IT Contractor notifies of job completion and supply BHRC Accounts Payable Officer with the invoice for payment process.

APPROVAL REQUIRED

The authorised IT Contractor is required to seek approval from the CEO in relation to the following:

- Renewal of domain names
- Renewal or upgrades of anti-virus software and other security software
- Renewal of a service contract which is substantially the same as the original one, in terms of price and service provision
- Purchasing equipment, software or services to meet an urgent, critical business need; for example, equipment designed to troubleshoot serious IT problems.

For all these situations, the authorised IT Contractor must provide receipts/invoices, and all other relevant documentation to Accounts Payable Officer for processing.

In relation to expenditure over the maximum amount of $5,000 (ex GST) to fix urgent problems, once the immediate problem is resolved, the authorised IT Contractor should provide an explanation of why usual purchasing procedures could not be followed and seek retrospective approval from the CEO.

Recording of ICT Equipment, Software and Services

The Governance Assistant in conjunction with the authorised IT Contractor records all new equipment, software and ICT services in an Excel spreadsheet/database titled ICT Equipment Database.

Information recorded in this spreadsheet includes information on purchase date, price, serial or other identification number, supplier/service provider details, physical location (e.g., which desk or staff member has it). For software, the information includes the number and expiry dates of licences and for ICT services, and the start and end dates of the contract.

The Governance Assistant will update the spreadsheet/database whenever changes occur to items; for example, change in location or users, lost, damaged or equipment that has been disposed of.

The authorised IT Contractor will also provide, normally via email, copies of all software and hardware licences purchased.

The Governance Assistant will provide a copy of the spreadsheet/database to the Finance Manager towards the end of the financial year for reconciliation against depreciation records.

ICT EQUIPMENT DISPOSAL

BHRC is committed to providing appropriate disposal methods to ensure all equipment is safely disposed of and organisational information is adequately protected.

This section provides guidance to BHRC staff members in disposing ICT equipment.

This section ensures that:

- BHRC ICT equipment is disposed of safely and appropriately.
- Council complies with ethical and environmental requirements in the disposal of ICT equipment.

- All staff understand their responsibilities in relation to disposing of ICT equipment.

ICT DISPOSAL PRINCIPLES

BHRC will ensure that ICT equipment is disposed in a manner which is:

- Transparent
- Cost-effective
- Environmentally sound
- Secure

ICT DISPOSAL TIMEFRAME

ICT equipment will be retired or disposed of when it fails, is ineffective, is beginning to cost more to maintain than the cost of purchasing a replacement item or is nearing the end of its effective lifecycle.

ICT DISPOSAL METHODS

ICT items can be disposed of in a range of ways, including sale, trade-in, donation to employees or other organisations, or recycle these redundant items.

A decision pertaining to how to dispose of equipment should be made on a case-by-case basis, through discussions between the authorised IT Contractor and the CEO, and taking into account the principles set out above, particularly the need for transparency.

Given the short life of most personal-use ICT items, BHRC generally will not consider a sale or trade-in on such items unless the anticipated profit to council will clearly be greater than the cost in the Governance Assistant's time spent arranging the sale or trade-in.

Recycling and Environmentally Responsible Disposal

Where items are not able to be passed on to staff or other organisations, the Governance Assistant in conjunction with authorised IT Contractor should make reasonable attempts to dispose of the item in a manner that does not contribute to landfill i.e., BHRC e-waste recycling program.

DELETION OF DATA PRIOR TO DISPOSAL

Before disposing of items (whether by providing to staff members for personal use, to another organisation or to e-waste recycling program) the authorised IT Contractor will professionally de-identify and securely erase all stored data so as to protect BHRC's privacy, comply with copyright law, and minimise the risk of data harvesting.

RECORDING DISPOSALS

The Governance Assistant in conjunction with the authorised IT Contractor will record all ICT disposals in the ICT Record Retention and Disposal Schedule/Register. All ICT equipment and tools disposals are recorded in the ICT Equipment Database.

Details to be recorded include:

- the date

- disposal method
- where/who the item goes to
- who authorised the disposal and;
- any income derived from that disposal

IT NETWORK

BHRC understands that a quality internal communication network is a crucial component to ensure communications and business are carried out inside the organisation to allow staff members to achieve organisational goals and outcomes.

The purpose of this section is to provide guidance to BHRC staff members into how the council assesses, manages and updates the internal network.

The following processes ensure that staff members are provided with a reliable and stable IT network.

This section ensures that:

- Staff members are able to work in a shared network environment;
- Organisation files are current, secure and up to date;
- Backup systems and procedures are in place to protect internal documentation;
- Private and confidential information is appropriately managed according to current legislation;
- The network is used in a manner that is consistent with Council's values, legal requirements, related policies, and code of conduct.

This section does not provide guidance on network/server or other equipment types and providers.

NETWORK SECURITY AND ANTI-VIRUS SOFTWARE

- The authorised IT Contractor is responsible for ensuring that the computer network is secure from external attacks. Firewalls and other cyber security protection and mitigation systems are installed for this purpose.
- The authorised IT Contractor is responsible for installing anti-virus software on the server(s) and every desktop computer. The software is set to auto-update virus definitions.
- The authorised IT Contractor is responsible for evaluating the performance of the anti-virus software at relevant intervals and renewing or switching to a new anti-virus software / licence, as required; all software information is available on the ICT Equipment Database.

NETWORK BACKUP

The authorise IT Contractor is responsible for ensuring that file server(s) are backed up regularly. The procedure for this backup is as follows:

- Server(s) are backed up ten (10) times per day on Monday to Friday into the backup cache drive.

- Date from the backup cached drive is grandfathered out to six (6) months and replicated both locally and to an offsite cloud storage provider daily with 256 bit encryption applied.
- The entire backup and disaster recovery system is monitored by the authorised IT Contractor daily.
- Once every three (3) months the authorised IT Contractor will conduct a test of each of the backup hard drives to check that they are correctly backing up all data.

SETTING UP USER ACCESS TO THE ICT SYSTEMS

When a new staff member (or other approved user) commences with BHRC, the Executive Assistant with CEO approval will inform the authorised IT Contractor and ask them to create a new login on council's network.

The Executive Assistant in conjunction with the authorised IT Contractor will undertake the following tasks:

- Ensure the new user has access to networked desktop computer and a desktop phone (if required);
- Create a new network user account with the appropriate access levels (see encryptions following);
- Ensure the new user has printer access;
- Create a new email account;
- Allocate a login for other internal systems;
- Assist the new user to set up their email access through Outlook Office 365 and to change passwords;
- Explain to the new user the network and filing matrix, how to use the phone, smart phone (if applicable) and set up voicemail facilities;
- Provide a copy of this policy and explain where to find information or seek assistance about particular issues;
- Support new users to use other internal ICT equipment and systems (if required).

DELETING A USER OR REMOVING THEIR ACCESS TO ICT SYSTEMS

When a staff member/or other user is no longer employed/contracted by BHRC, or when directed by the CEO to disable a current user's account, the Executive Assistant in conjunction with the authorised IT Contractor is to undertake the following tasks:

- Disable the user's access/delete their login details in relation to the computer network and other internal systems;
- Consult with the CEO as to whether emails to the former user should be forwarded to another staff member or whether the account should be deleted;
- Remove the user's name from the internal address book.

LEVELS OF ACCESS

BHRC's server(s) consists of a number of network drive(s) with certain access restrictions. The authorised IT Contractor are to ensure that individual staff members or other users are provided with the appropriate levels of access.

UNAUTHORISED ACCESS TO OR INTERFERENCE OF DATA

Unauthorised access or deliberately modifying or damaging BHRC data is a violation of Council's Code of Conduct and Confidentiality Agreement staff members sign at the commencement of their employment; and may result in criminal charges or legal proceedings.

MAINTENANCE OF ICT EQUIPMENT

Staff are required to take reasonable precautions to protect IT equipment from damage, loss or theft. If staff members want to change or modify equipment that is provided to them by council for work purposes, they must seek approval from their CEO.

General maintenance of ICT equipment is the responsibility of the authorised IT Contractor to the extent of recommendation, which will then be assessed and authorised by the CEO for action.

PASSWORDS

BHRC is committed to providing IT equipment, services and platforms that are secure and provide appropriate expectations regarding the safe use of passwords when working on council ICT equipment and tools.

The purpose of this section is to provide guidance to BHRC staff members on the creation and use of safe passwords in order to increase the council's IT network security and reduce the risk of external intrusion.

The following processes ensure that staff members, are aware of their responsibilities and the steps to create strong and secure passwords.

This section ensures that:

- Internal network and related document security and privacy is not compromised
- Staff members' privacy is protected
- Staff members are aware of their password responsibilities

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of BHRC's resources. All system users are responsible for taking the steps outlined below to select and secure their passwords.

The sharing of passwords is to be avoided and not standard practice.

AUTHORISED IT CONTRACTOR RESPONSIBILITIES

The authorised IT Contractor allocates initial passwords to each new user for access to the network, email, and/or other relevant systems. The authorised IT Contractor must then advise new users to change their passwords and refer them to this policy for advice on choosing passwords.

The authorised IT Contractor cannot reset or access users' accounts, or change their passwords, unless expressly authorised by the user or by the CEO. The CEO may authorise access where there has been a breach in the Code of Conduct and the CEO requires information to appropriately manage the incident.

COPYRIGHT AND SOFTWARE LICENCES

BHRC is committed to comply with copyright legislation, licences and user responsibilities in regard to equipment, software and services purchased by or provided to council in order to fulfil its obligations and duties.

The purpose of this section is to provide guidance to BHRC staff members on their responsibilities in using copyright material and licences appropriately, as part of their role within the council.

This section ensures that:

- Employees comply with current legislation and acknowledge copyright work, material and services
- Employees are supported to provide consistent and quality online experiences
- Organisational research, programs, services and activities are consistent with Council's values, legal requirements, related policies and code of conduct

This section does not provide guidance on research.

The Copyright Act 1968 (Cth) protects the rights of creators of material, including software, as well as documents, files or pictures on the internet. In addition, software and application developers routinely issue licences or terms and conditions that users are required to comply with.

BHRC staff members are required to conform to the requirements of the Copyright Act 1968 (Cth) and licences for software use.

SOFTWARE LICENCES

When BHRC computing or networking resources are being used, copying of software in a manner not consistent with the vendor's licence is strictly forbidden. If users are not sure what is and what is not permitted under a particular licence, they should speak to the authorised IT Contractor or the vendor.

When council disposes of equipment which contains software (other than the operating system) that is licensed to BHRC, the authorised IT Contractor is to remove that software. Refer to **ICT Equipment Disposal** section of this policy for more information.

It is not permitted for any reason, to use pirated or illegal software or licences within the boundary of the corporate ICT network.

USE OF MATERIALS FROM THE INTERNET

Reproduction of materials available over the internet must be done only with the written permission of the author or owner of the document.

Permission is sometimes granted on the website with a statement that declares you may download a document for personal or non-commercial use. In the absence of such a statement, users should email a request for permission to use it. The right to use the material may be limited by the terms of the permission granted, and/or by any conditions that the copyright owner imposes.

Unless permission from the copyright owner(s) is obtained, making copies of material or saving material to a hard drive is unlawful, unless it for a specific list of purposes and it is a "fair dealing".

If BHRC staff are in doubt as to whether they can download and/or copy material from the internet, they should consult their Compliance Officer.

STAFF USE OF COMMUNICATION TOOLS

BHRC understands that communications tools such as phone, email, internet and social media applications have become essential component parts in the way communications and business are carried out to relate with communities, clients, staff members and other organisations.

The purpose of this section is to provide guidance to BHRC staff members on using these tools as practical instruments to engage with the sector and its stakeholders, improve services participation, enhance transparency and fully realise council's goals and strategic outcomes.

The following processes ensure that use of communication tools is of a consistent high quality, are collaborative, appropriate, transparent and that users are accountable using the tools as part of their duties.

EMAIL USE

Employees may use email access provided by the council for any work related purposes of BHRC.

Emails related to the core business of BHRC will be stored within Microsoft Office365 cloud environment and replicated to a third party cloud storage provider.

Employees can generally expect that the subject and recipients of email may be monitored intermittently.

BHRC reserves the right to read and take action on employee emails if there is reasonable evidence that an employee is breaching this policy.

Email can be subject to production in litigation or other investigations.

Email Signature

The Corporate Image of the Council as detailed in the Corporate Style Guide sets out the recommended font and text for staff members' email address block, signature and other inclusions.

Prohibited Use of Email

The use of BHRC email in the following contexts is strictly prohibited:

- Reading or sending messages from another user's account, without BHRC authorisation
- Altering or copying a message or attachment belonging to another user without the permission of the creator of the message/attachment
- Subscribing to list servers and distribution lists unless they are directly related to your work or permitted by your CEO
- Exchanging information in violation of copyright laws

- Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised) course of their duties
- Creating or exchanging messages that are offensive, harassing, obscene or threatening
- Promoting websites containing objectionable or criminal material.
- Conducting a business or conducting illegal activities
- Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email.

MEDIA

Social Media

BHRC recognises the use of social media for open dialogue and the exchange of ideas where it is beneficial for individuals in their work or research capacity.

In using social media, staff members are asked to be considerate, to be transparent and to understand that even when posting in a personal capacity, they may be viewed as representative of BHRC, and therefore their actions can impact upon council's reputation. For further information refer to the Code of Conduct.

Website

BHRC has website which provides information to the general public about the council and it's services. BHRC is committed to promoting the council in an accessible, transparent and user friendly manner.

The purpose of this section is to provide broad guidance to BHRC Executive Assistant to the CEO on the council's website management and the process for contributing content to the website.

This section ensures that:

- Online communication tools support the council's goals and outcomes
- Executive Assistant contribute appropriately to the council's website
- The council's website is reliable, secure and up to date

Website Hosting and Security

BHRC contracts an external Website Support Company who is responsible for renewing BHRC website hosting services through an online registration process, the details of which are contained in the ICT Equipment Database.

Access to Website Content

The Executive Assistant is responsible for maintaining and keep council website up to date with current and new content and access the website via website content management system provided by the authorised Website Support Company with user and password details provided by the authorised website support company.

INTERNET USE

Employees may use internet access provided by council for any work-related purposes. BHRC in conjunction with the authorised IT Contractor can monitor logs of internet usage which may reveal information, such as which servers (including websites) have been accessed by the employee, and email addresses used.

Employees will ensure that the internet is used in a manner consistent with the Code of Conduct and as part of the normal execution of an employee's job responsibilities. Internet users will not compromise the privacy of their password by sharing it with other or exposing it to public view.

Prohibited Use of Internet

Staff members are strictly prohibited from using BHRC's internet facilities to undertake the following activities:

- Visiting websites containing objectionable or criminal material
- Gambling, gaming, conducting a business or conducting illegal activities
- Installation of software without BHRC authorisation
- Creating or exchanging messages that are offensive, harassing, obscene or threatening
- Creating, storing or exchanging information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies)

PHONE USE

Employees may use phones provided by council for any work-related purposes and will endeavour to make all telephone calls as brief as possible.

Employees will answer the phone courteously with an agreed greeting message and respond appropriately to callers' requests.

Mobile Telephones

Employees are responsible and accountable for the use, safekeeping and security of BHRC mobile phones issued on a loan basis to employees and which remain the property of council.

INTERNAL CLIENT DATABASE

BHRC has an internal client database containing details about all its clients. Basic information about clients is extracted by allocated and authorised staff members to perform their duties.

The purpose of this section is to provide guidance to BHRC staff members on using the internal client database processes as a practical instrument to manage client information, treatment and outcomes.

These processes also:

- Are recognised as an internal part of council's client support
- Enable holistic service provision, collaboration and engagement with the sector to achieve client outcomes

- Support accountable practices and reliable data

This section ensures that staff members:

- Use responsible and accountable processes to support clients
- Maintain accurate client records
- Use client information as required to complete their duties

ACCESS AND MAINTENANCE

The Executive Assistant in conjunction with Finance Manager and CEO, provides authorised staff members with login and initial password which allows them to use and update the database. Access levels are managed by the Executive Assistant according to staff roles and positions.

UPDATING RECORDS

All authorised staff members with client responsibilities are required to update information about clients, for example:

- Creating new records
- Updating contact details
- Adding changes to the client's file notes

REPORTING AND VERIFICATION OF DATA

The Executive Assistant will:

- Support staff members to generate reports as required
- Be able to generate reports for staff members with the main purpose of complying with accounts, usage etc. reporting requirements
- Not create, delete or edit records without the written authority of the staff member who created or edited a record
- Monitor the quality of the data collected, and work with staff members to improve data input

DATABASE SECURITY

In recognition of the sensitivity and confidentiality of the information contained in the Internal Client Database, BHRC has in place a high level of database security and several backup measures.

The Internal Client Database is stored on the server PDC-BHRC which is located in the secure communications room. The backup and disaster recovery system conducts ten (10) backups every one (1) day onto a removable onsite hard drive called backup cache drive located in HV-BHRC.

The authorised IT Contractor regularly monitors the security of the database; for example, checking access logs and investigating unusually large transfers of data. The authorised IT Contractor will advise the CEO, should they identify any suspicious activity that they deem requires further investigation.

DATABASE IMPROVEMENT OR REDEVELOPMENT

The Executive Assistant in conjunction with authorised IT Contractor or Finance Manager will ensure the data sets used by the Internal Client Database are updated in line with reporting requirements.

Where BHRC identifies, that major changes are required to the database which cannot be undertaken by the Executive Assistant, the authorised IT Contractor is required to prepare a comprehensive project brief in consultation with the Executive Assistant and Finance Manager, to be approved by the CEO. The development brief will set out the budget, and responsibilities for project management of the database development, including supervision of the contractors, etc.

RELATED DOCUMENTS

INTERNAL:

Supporting Documents

- Electronic Records Matrix
- Record Retention and Disposal Schedule
- Recordkeeping Disaster Recovery Plan 2018-2023
- Recordkeeping Procedure Manual 2018
- ICT Equipment Database
- ICT Record Retention and Disposal Schedule/Register

Related Policies

- Code of Conduct
- Risk Management Policy
- Purchasing Policy

EXTERNAL:

Legislation

- Privacy Act 1988
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- State Records Act 2000
- Copyright Act 1968 (Cth)
- Fair Work Act 2009 (Cth)
- A New Tax System (Goods and Services Tax) Act 1999 (Cth)
- Electronic Transactions Act 2011 (WA)

DOCUMENT CONTROL				
DOCUMENT OWNER			Chief Executive Officer	
RESPONSIBLE FOR REVIEW			Governance Assistant	
REVIEW SCHEDULE: Biennial			REVIEW DATE: June 2023	
DATE	DOCUMENT	VERSION	DESCRIPTION OF CHANGE	RESOLUTION No.
10/06/2021	ICT POLICY	DRAFT		