TITLE:	Information, Communications & Technology (ICT) Resources Policy		
DIVISON:	Corporate Policy		
ADOPTED BY:	Council		
DATE OF ADOPTION:	25 January 2018	**DATE OF REVIEW:**	1 January 2020
MOTION NUMBER:	OC 12/18		
POLICY NUMBER:	CP000054		
AUTHORISED:	Chief Executive Officer		

THIS POLICY APPLIES TO:
All employees of the Barkly Regional Council, Elected Members and Authorised Users of Barkly Regional Council ICT Infrastructure.

PURPOSE AND OBJECTIVES

The aim of all policy is for Councillors to provide strategic input into the effective operational framework of the organisation under S.11 of the Local Government Act

The Barkly Regional Council's Information, Communications and Technology (ICT) resources are provided to support and enhance the Council's activities and operations.

This policy informs users of Barkly regional Council ICT resources of the rights and responsibilities.

This policy also applies to the use of information that may be accessed via ICT resources.

This policy must be read in conjunction with all Procedures for the Acceptable Use of ICT Resources and associated Procedures and Guidelines related to specific ICT-related hardware, software and applications.

DEFINITIONS, TERMS, ACRONYMS

Account/Sign-In - access provided by Barkly regional Council to any ICT resource or any non-Barkly Regional Council ICT resource utilised for Barkly Regional Council purposes.

BRC – Barkly Regional Council

ICT - Information Communication Technology. ICT products and services are defined as all types of technology (data, voice, video etc) and associated resources which relate to the capture, storage, retrieval, transfer, communication or dissemination of information through the use of electronic media.

User - all staff, elected members, contractors, third parties, and all other people who legitimately access Barkly Regional Council's systems and/or networks

Other Entities - External organisations which may provide ICT solutions (e.g. Microsoft), host services such, and Barkly Regional Council affiliated organisations and committees.

POLICY SCOPE/COVERAGE

This policy applies to all Users of BRC's ICT resources.

The policy also applies to anyone connecting non-BRC or affiliated (including personally-owned) ICT equipment (e.g. laptops) to BRC's network.

POLICY STATEMENT

BRC sets policy on the acceptable use of BRC ICT resources in respect of provision of resources, access to resources, responsible, ethical equitable and legal use of resources, security and privacy, compliance and breaches and responsibilities. Policy details on each of these aspects are outlined in the sections below.

1. Provision of ICT Resources

ICT Resources encompass infrastructure, equipment, software, and facilities including technologies such as computers, smart phones, the Internet, broadcasting technologies (radio and television), and telephony. ICT resources include:

- All networks, hardware, software and communication services and devices which are owned, leased or used under licence by BRC including BRC's service provision and administrative systems;
- Computing facilities and information resources maintained by Other Entities , but available for use through an agreement or agreements with BRC; and
- Web pages hosted on BRC ICT Resources.

BRC recognises the importance of ICT and provides access to Users for Council and other authorised purposes according to need and available resources. Usage is subject to the conditions set out in this policy and associated procedures.

Access to ICT resources through the BRC network is a cost to the Council and is not provided to Users unconditionally.

BRC does not permit its ICT resources to be used for unauthorised activities.

BRC cooperates with network providers, legal authorities of the Territory and Commonwealth, and the international community to provide a reliable and trustworthy service.

Whilst BRC respects the privacy of Users of ICT Resources, BRC reserves the right to monitor User activity and take appropriate action if misuse of resources is identified. Monitoring for misuse of BRC ICT Resources must be authorised by the Executive Leadership Team.

Software

BRC requires that Users and Departmental Units use and install software in compliance with licence terms and conditions.

The same purchasing rules apply to online software purchases as purchases using traditional mechanisms.

It is a criminal offence if an individual makes an infringing copy of software with the intention of obtaining a commercial advantage or profit and if the individual knows or ought reasonably to know that the copy is infringing copyright.

Installation of privately purchased and owned software on BRC systems is not advised. If this is necessary, the owner must contact either their local Software Licensing Point of Contact or the BRC IT Departments to have the software registered and to check the

installation is allowed under the license terms. Proof of purchase is required, consisting of the license certificate and original media, and the invoice if it is available.

Portable Devices

Portable devices such as mobile phones, satellite phones, mobile internet services, and Portable Data Advices (Tablets) may be provided to Users.

Access to such devices is on as needs basis and will be approved by the Executive Leadership Team.

Temporary access is will also be available from a resource pool maintained by the Information Technology Department.

Executive Leadership Team approval of all purchasing of portable devices is mandatory as outlined in the Delegations Manual.

Computing Resources for BRC Libraries

BRC will continue to provide library computer facilities in line with equity principles and funding requirements.

Information Management

Users must take appropriate steps to ensure the security, confidentiality, and integrity of all BRC related information stored or received, including measures to prevent loss of information.

Records Management

It is the responsibility of staff, committee members, appointed members and elected members to submit to the relevant records storage system any information that is (or is reasonably likely to be at that time) a Council record or part of a Council record.

Cloud/Shared Network Computing

It is the responsibility of administration system owners to follow all applicable legislative guidelines when implementing a cloud computing solution for administration systems. Reference should be made to the Department of Defence Cloud Computing Security Considerations. Administration system owners should consider the checklist in this document when conducting an analysis of a cloud computing solution.

2. Access

A BRC User account and email address is provided for access to BRC ICT Resources.

Access to the Internet must be via an authorised account associated with the User or to the corresponding BRC authorised and registered application. Conditions may also apply for Users who are under 18.

Users must protect the security and integrity of their access e.g. account, password and equipment on which this is saved.

Users must keep their passwords confidential and must not share them with anyone else, or reveal them to anyone else.

Accounts (including internet accounts) must not be transferred or in any other way made available for the use of a person other than the account holder.

You must not use your BRC Sign-in, including password or username, for systems external to BRC unless it is for authorised BRC purposes.

If an account holder knows or suspects their account has been used by another person, or suspects their password has been revealed (including lost or stolen passworded ICT equipment), the account holder must immediately change their password.

Staff are required to change their password at least once every 2 months.

BRC reserves the right to remove or limit access to ICT resources, and to remove or limit access to material and resources stored on BRC-owned computers or other resources. Changes to access must be directed to the Executive Leadership Team member responsible for Information Technology Services.

Access to all resources utilising a BRC Sign-in will be subsequently terminated when Users cease association with BRC (e.g. when a staff member is no longer employed).

Access will cease immediately the staff member is terminated in the Human Resources system.

Supervisors must make arrangements to terminate access to other systems not utilising a central BRC Sign-in.

3. Responsible, Ethical, Equitable and Legal Use of ICT Resources

BRC requires all Users of its ICT resources to do so in a responsible, ethical, equitable and legal manner and in accordance with all BRC Policies, Procedures and Codes of Conduct.

Legal and policy framework

Users of BRC ICT resources must be aware that use of these resources is subject to the full range of Australian laws as well as any other relevant BRC policies and statutes. This includes (but is not limited to) areas such as copyright, breach of confidence, defamation, privacy, contempt of court, bullying and cyber-bullying, harassment, vilification, anti-discrimination, willful damage and computer hacking.

Users should be aware that access to some third party applications and content has separate contractual arrangements and terms and conditions which may apply over and above this policy.

Publishing

BRC media policy guidelines apply to all material published using BRC resources.

Carrying of advertising or commercial logos on BRC web pages requires prior permission from the Chief Executive Officer.

Limited personal use

The use by BRC Staff of ICT resources for personal purposes is not generally permitted unless such use is kept to a minimum. Limited personal use is defined as:

• incurs minimal additional expense to the Council;

• is infrequent, brief and not during paid working hours;

• does not interfere with the operations of the Council; and

• does not violate any Council policy or related State/Federal legislation and regulation.

4. Security and Privacy

Access to information through ICT Resources will only be provided if there is a legitimate need.

Users should be aware that legal or other requirements may necessitate access, retention, inspection and release of electronic files and communications (including email) held on or transferred through the BRC's systems (including after termination). This includes authorised

monitoring of User activity when investigating possible misuse and may include any personal information held on BRC ICT Resources.

Users who have authorised access to private information about staff, appointed members or elected members, or confidential information of the BRC must respect the privacy of others and maintain the confidentiality of the information to which they have access in accordance with privacy laws and any BRC policies.

5. Compliance and Breaches

Notifying and handling of breaches

Users who become aware of possible breaches of this policy must report it to either:

- their supervisor or manager;
- their Directorate Head;
- the Executive Leadership Team; or
- the Chief Executive Officer.

The Executive Leadership Team is responsible in the first instance for handling potential breaches. This could result in revocation of access.

Formal disciplinary action for staff will occur in accordance with the Misconduct/Serious Misconduct clauses as outlined in the Enterprise Agreement or any other applicable Instrument of Employment.

BRC may refer serious matters to the appropriate external authorities which may result in civil or criminal proceedings.

BRC has an ethical and statutory obligation to report illegal activities and corrupt conduct to appropriate authorities.

Penalties associated with breaches

Penalties for misuse of ICT resources may range from loss or restriction of access to accounts, to formal disciplinary action including the termination of employment or in some more serious instances criminal or civil proceedings. This could include financial penalties.

6. Responsibilities

Directorate Holders and Executive Leadership Team Members are responsible for compliance with and communication of BRC ICT policies.

The Executive Leadership Team Members are responsible for Information Technology Services has the responsibility for coordinating the implementation of this policy and any associated documents.

EVALUATION AND REVIEW

This Policy is to be reviewed every two (2) years, and may be reviewed at other times at the discretion of Chief Executive Officer.