Information, Communication and Technology (ICT) and Social Media Policy

Policy Number	KASC-ADMIN-011
Responsible Manager	Chief Executive Officer
Head Policy	Code of Conduct
Legislation	Local Government Act 2009 Local Government Regulation 2012
Associated Documents	KASC Equipment Issue Form CCTV Policy
Approval Date	17 August 2021

1. Definitions and Terms

1.1 In this policy:

Council	Means Kowanyama Aboriginal Shire Council
Confidential Information	Includes but is not limited to trade secrets of KASC; non-public information about the organisation and affairs of KASC such as: pricing information (including internal cost and pricing rates), production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; contractual arrangements with third parties; tender policies and arrangements; financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from KASC or obtained in the course of working or providing services to KASC that is by its nature confidential.
Computer Surveillance	Means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of KASC's Information, Communications and Technology (ICT) systems and devices (including, but not limited to, the sending and receipt of emails and the accessing of websites).
Information, Communications and Technology Systems and Devices	Includes all KASC internet, email and computer facilities which are used by Users, inside and outside working hours, in the workplace of KASC (or a related corporation of KASC) or at any other place while performing work for KASC (or a related corporation of KASC). It includes, but is not limited to, desktop computers, laptop computers, Blackberrys, Palm Pilots, Personal Digital Assistants (PDAs), other handheld electronic devices, smart phones and similar products, and any other means of accessing KASC's email, internet, and computer facilities, (including, but not limited to, a personal home computer which has access to KASC's ICT systems).

Intellectual Property	Means all forms of intellectual property rights throughout the world including copyright, patent, design, trademark, trade name, and all Confidential Information and including know-how and trade secrets.
Person	Includes any natural person, company, partnership, association, trust, business, or other organisation or entity of any description and a Person's legal personal representative(s), successors, assigns or substitutes.
SPAM	Is a term used describe irrelevant or unsolicited messages sent over the internet, usually via mail and typically to a large number of users for the purposes of advertising, phishing or spreading malware and viruses.
User	Applies to all employees, contractors, and councillors of Kowanyama Aboriginal Shire Council.

2. Acronyms and Abbreviations

2.1 In this policy:

KASC	Means Kowanyama Aboriginal Shire Council
ICT	Means Information, Communications & Technology
PDA	Is a Personal Digital Assistant
URL	Means Universal Retrieval Location

3. Purpose of the Policy

3.1 This policy sets out the standards of behaviour and conduct expected of persons when using KASC's ICT systems and devices and when engaging in communications within the organisation and on social media.

4. Application of this Policy

4.1 This policy applies to all users of the KASC ICT systems and devices.

4.2 The policy also applies to users who contribute to external websites and identify themselves as associated with KASC.

5. Use of ICT Equipment

5.1 Users are permitted to use KASC's ICT systems and devices for limited and reasonable personal use. Any personal use of KASCs ICT systems and devices must not impact upon the User's work performance or KASC resources and must not violate any KASC policy.

5.2 A User must not use KASC's ICT systems and devices for personal use if that use interferes with the efficient business operations of KASC.

5.3 KASC gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any User while using KASCs ICT systems and devices for the User's personal purposes.

6. Requirements For Users

6.1 Users must comply with the following rules when using KASC's ICT systems and devices:

a) Users must use their own KASC allocated username/login code and/or password when accessing the KASCs ICT systems and devices.
b) Users in possession of KASC electronic equipment must always handle the equipment in a responsible manner and ensure that the equipment is kept secure.
c) Users should always protect their username/login code and password information and not divulge such information to any other person.
d) Users should ensure that when not in use or unattended, the computer system or mobile devices is shut down or locked.
e) A disclaimer is automatically included in all KASC emails and must not be removed.
f) If a User receives an email which the User suspects contains a virus, the User should not open the email or attachment to the email and should immediately contact Council's nominated IT provider.
g) If a User receives an email (including an image, text, materials, or software) that is in breach of this policy, the User shall immediately report the matter to Council's nominated IT provider and Governance and Operations. The User must not forward the email to any other Person.

7. Prohibited Conduct

7.1 Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on KASC's ICT Systems and devices that:

a) is obscene, offensive, or inappropriate. This includes text, images, sound, or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL). For example, material of a sexual nature, indecent or pornographic material;
b) causes (or could cause) insult, offence, intimidation or humiliation;
c) may be defamatory or could adversely impact the image or reputation of KASC (a defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people);
d) is illegal, unlawful or inappropriate;
e) affects the performance of, or causes damage to KASC's ICT systems and devices in any way;
f) gives the impression of or is representing, giving opinions, or making statements on behalf of KASC without the express authority of KASC.

7.2 Users must not transmit or send KASC's documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

7.3 Users must not use KASC's ICT systems and devices to:

a) violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into by using KASC's computing facilities, except as permitted by law or by contract with the owner of the copyright;
b) create any legal or contractual obligations on behalf of KASC unless expressly authorised by KASC;
c) disclose any confidential information of KASC or any customer, client or supplier of KASC unless expressly authorised by KASC;
d) install software or run unknown or unapproved programs on KASC's ICT Systems and Devices. Under no circumstances should Users modify the software or hardware environments on KASC's ICT Systems and Devices unless expressly authorised to do so;
e) gain unauthorised access (hacking) into any other computer within KASC or outside KASC, or attempt to deprive other Users of access to or use of KASC's ICT systems and devices;
f) send or cause to be sent chain or SPAM emails in any format;

g) use KASC ICT systems and devices for personal gain, for example, running a personal business.

7.4 Users must not use another User's KASC ICT Systems and Devices (including passwords and usernames/login codes) for any reason without the express permission of the User or an authorised KASC employee such as the CEO or Executive Manager.

7.5 If a user has divulged their logon credentials, either advertently or inadvertently, to any other user or person, they must change their password details as soon as possible after they become aware of those details being divulged.

8. KASC ICT Equipment Issue

8.1 All KASC ICT Systems and devices, including laptops, mobile phones, cameras, and other devices that are issued to users require a KASC Equipment Issue Form to be signed by the user and returned to the Executive Manager of Human Resources.

8.2 The KASC Equipment Issue Form details the responsibilities (in addition to this policy) of the user while they are in possession of KASC ICT systems and devices.

9. Blocking Access to KASC ICT Systems and Devices

9.1 KASC reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a User, or access to an internet website by a User, if the content of the email or website is considered:

a) obscene, offensive, or inappropriate. This includes text, images, sound, or any other material, sent either in an email message or in an attachment to a message, or through a link to a website. For example, material of a sexual nature, indecent or pornographic material;
b) causes or may cause insult, offence, intimidation or humiliation;
c) defamatory or may incur liability or adversely impacts on the image or reputation of KASC. A defamatory message or material is a message or material that is insulting or lowers the reputation of a Person or a group of people;
d) illegal, unlawful or inappropriate;
e) to have the potential to affect the performance of, or cause damage to or overload KASC Computer Network, or internal or external communications in any way;
f) to give the impression of or is representing, giving opinions or making statements on behalf of KASC without the express authority of KASC.

9.2 In the case that an email is prevented from being delivered to or from a User, the User will receive a prevented delivery notice. The notice will inform the User that the delivery of the email has been prevented. The notice will not be given if delivery is prevented in the belief that:

a) the email was SPAM, or contain potentially malicious software; or
b) the content of the email (or any attachment) would or might have resulted in an unauthorised interference with, damage to or operation of any program run, or data stored on any of KASC's equipment; or
c) the email (or any attachment) would be regarded by a reasonable person as being, in all the circumstances, menacing, harassing or offensive.

9.3 KASC is not required to give a prevented delivery notice for any email messages sent by a User if KASC is not aware (and could not reasonably be expected to be aware) of the identity of the User who sent the e-mail or is not aware that the e-mail was sent by the User.

10. Types of Surveillance in KASC's Workplace

10.1 On a continuous and ongoing basis, KASC will carry out Computer Surveillance of any User at such times of KASC's choosing and without further notice to any User.

10.2 Computer Surveillance occurs in relation to:

a) storage volumes;
b) websites accessed;
c) download/upload volumes;
d) suspected malicious code or viruses;
e) emails - the content of all emails received, sent, and stored. (This also includes emails deleted from the inbox); and
f) hard drives and external storage devices - KASC may access any hard drive on the Computer Network.

10.3 KASC retains logs, backups, and archives of computing activities, which it may audit. Such records are the property of KASC, are subject to State and Federal laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

10.4 On a continuous and ongoing basis, KASC will carry out Mobile Phone Surveillance of any KASC issued mobile phone at such times of KASC's choosing and without further notice to any User. Mobile Phone surveillance includes

a) Data Usage
b) Call Usage, including numbers dialed, and length and cost of calls.
c) Location of call origin
d) Monthly expenditure.

11. KASC Use of Surveillance Records

11.1 KASC may use and disclose the Surveillance Records where that use, or disclosure is:

a) for a purpose related to the employment of any employee or related to KASC's business activities; or
b) use or disclosure to a law enforcement agency in connection with an offence; or
c) use or disclosure in connection with legal proceedings; or
d) use or disclosure reasonably believed to be necessary to avert an imminent threat of serious violence to any Person or substantial damage to property.

11.2 Use or disclosure of Surveillance Records can occur in circumstances of assault, suspected assault, theft, or suspected theft of KASC's property (or that of a related corporation of KASC) or damage to KASC's equipment or facilities (or that of a related corporation of KASC). It can also occur to ensure KASC's ICT equipment is being accessed and utilised appropriately and in accordance with relevant KASC policies and procedures.

12. Excessive Use of Equipment

12.1 If an employee or councilor uses any council ITC equipment or services excessively and incurs cost to council, they are liable for the costs and must repay costs to council.

13. ICT Security & Device Protection

13.1 Users are responsible for the physical and electronic/online security and protection of the ICT equipment issued to them. Any security threats or actual security events must be reported to the user's Executive Manager.

13.2 Physical security threats or events include:

a) Theft or attempted theft of any KASC ICT equipment.
b) Access or attempted access to the KASC ICT environment using another user's logon
c) Access or attempted access to KASC ICT network or devices for any unlawful purpose or any purpose that is not in accordance with any KASC policy or procedure (including KASC Code of Conduct).

13.3 Users must take all reasonable steps to care for the ICT equipment issued to them. This includes:

a) The use of any protective equipment that is issued with the device, such as a laptop bag or mobile phone case.
b) No use of unnecessary force or inappropriate manual handling such as throwing a device or rough handling of the device.
c) Ensuring the device is not exposed to bad weather or environment conditions and is regularly cleaned from dust and dirt.

14. Social Media

14.1 Users have the right to participate in public and political debate but in some cases, their responsibilities may limit their ability to participate fully in public discussions, including on social media. Kowanyama Aboriginal Shire Council users must comply with the following standards:

a) Users must not disparage or make any adverse comment about Kowanyama Aboriginal Shire Council, any policy or decision of Council or any of Kowanyama Aboriginal Shire Council's related entities, employees, contractors and other Kowanyama Aboriginal Shire Council officials or any other person or organisation providing services to or on behalf of Council.
b) Users must not harass, bully, intimidate or threaten another employee, councillor, contractor or other Kowanyama Aboriginal Shire Council official (or a person the user knows to be a relative or associate of a Kowanyama Aboriginal Shire Council official) when contributing on a social media site or platform.
c) Users, who can be identified as a representative of Kowanyama Aboriginal Shire Council, must not use social media networking sites and social media platforms to send, post or otherwise publish inappropriate content, including:
    - obscene messages/material
    - racially and/or sexually harassing messages/material
    - sexually explicit messages/material.
d) Must only disclose publicly available information and must not disclose confidential information.
e) Ensure that any information they post online about Kowanyama Aboriginal Shire Council, or a related entity of Council is informed and factually accurate and will not adversely impact Council.
f) Unless expressly authorised to do so by Kowanyama Aboriginal Shire Council, a user must not transmit or send Kowanyama Aboriginal Shire Council documents, emails, or text messages to any external parties or organisations.
g) If the user subsequently discovers a mistake on their blog or social networking entry, they are required to immediately inform Kowanyama Aboriginal Shire Council and then take steps authorised by Kowanyama Aboriginal Shire Council to correct the mistake. Any alterations should indicate the date on which the alteration was made.

15. Cyber Security

15.1 All care must be taken by users to avoid all cyber security incidents or events. Cyber security threats to KASC ICTs can occur in various ways in both target and non-targeted attacks.

15.2 Any potential or actual cyber security threat must be reported to the user's Executive Manager and forwarded to the KASC Governance & Operations team for investigation.

15.3 All reported cyber security threats must be taken seriously and managed with appropriate priority and urgency by all users, managers and those responsible for KASC ICT.

15.4 Some examples of a Cyber Security threat include:

a) Suspicious or malicious emails and attachments.
b) Suspicious or malicious links in emails and email attachments.
c) Unwarranted and suspicious phone calls to KASC mobile phones.
d) Unwarranted and suspicious text messages to KASC Mobile phones or computer messaging applications.
e) Request to submit or forward on any KASC ICT user information such as passwords or user details.
f) Any request for a user's password to a KASC ICT system, computer, or mobile device.

16. ICT Standards

16.1 Where possible and viable, KASC will utilize systems and software that comply with the requirements of ISO 27001 - Information Security Management Systems.

17. Essential Eight Activities

17.1 KASC shall also aim to meet the intent of the Commonwealth Government's Australian Cyber Security Centre Essential Eight mitigation strategies. The Essential Eight mitigation strategies have been developed to assist organisations to mitigate cyber security incidents caused by various cyber threats.

17.2 The guidance included in the Essential Eight activities addresses targeted cyber intrusions (i.e., those executed by advanced persistent threats such as foreign intelligence services), ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise' and industrial control systems.

18. Breaches

18.1 Breaches of this policy should be reported to the Executive Manager Governance and Operations, or in the case of a breach by the Executive Manager Governance and Operations, to the Chief Executive Officer or the Mayor.

18.2 In the case of breaches by a Councillor, Mayor or Deputy Mayor, breaches should be reported to the Chief Executive Officer.

19. Policy Review

19.1 The policy is to be reviewed in accordance with the Policy Framework Policy – KASC-ADMIN-001.

19.2 Kowanyama Aboriginal Shire Council reserves the right to vary, replace, or terminate this policy from time to time.

20. Approval

20.1 This policy was duly authorised by the Chief Executive Officer on 17 August 2021 as the Kowanyama Aboriginal Shire Information, Communication and Technology (ITC) and Social Media Policy and shall hereby supersede any previous policies of the same intent.