Information Technology Procedure - Personal Data Breach

Section 1 - Purpose

(1) This procedure supports the Information Technology Policy and:

a. outlines responsibilities of staff and students in response to suspected or identified breaches of personal information held by Charles Sturt University (the University)
b. determines if a personal data breach constitutes an eligible data breach that must be reported to the Office of the Australian Information Commissioner (OAIC) in compliance with the Privacy Act 1988
c. outlines the steps and responsibilities in reporting eligible data breaches to the OAIC, described as the Notifiable Data Breaches scheme.

(2) This procedure is a key component of the University's data breach response plan. The data breach response plan outlines how the University will respond to, and initiate improvements in the University's response to, personal data breaches.

Scope

(3) This procedure applies to all University staff, students and other relevant parties including visitors, contractors and associated bodies who own, manage, access or use the University's information and communications technology (ICT) services.

(4) This includes all:

a. ICT systems and data attached to University computer or telephone networks
b. University systems
c. communications sent to or from the University
d. data owned by the University, either internally or on systems external to the University network.

Section 2 - Policy

(5) See the Information Technology Policy

Section 3 - Procedure

Reporting a data breach

(6) All University staff must report any suspected or known breaches of personal information held by the University to the IT Service Desk as soon as possible.

(7) All University students must report any suspected or known breaches of personal information held by the

University to Student Central as soon as possible.

Containing a data breach

(8) The suspected or known breach must be promptly contained to minimise scope and impact of breach.

(9) The IT Service Desk will:

a. record the incident
b. where possible, contain the data breach
c. escalate the incident to the ICT Security Team.

Preliminary data breach assessment

(10) The ICT Security Team will complete a preliminary assessment to determine the criticality and eligibility of the incident as soon as possible.

(11) On completion of the preliminary assessment:

a. if it is determined that there has been an eligible data breach, the ICT Security Team must notify the Data Breach Response Team with the results including the:
    i. likelihood of causing serious harm to individuals
    ii. number of individuals impacted
    iii. nature and scope of the data breach.
b. if it is determined that there has not been an eligible data breach, ICT Security Team must:
    i. consider how the data breach occurred
    ii. recommend enhanced personal information security measures
    iii. seek endorsement of recommendations from the Data Breach Response Team
c. if it is unable to be determined that there has been an eligible data breach, ICT Security Team must:
    i. complete a more detailed risk assessment within a 30 day period in order to determine if it is an eligible data breach
    ii. on completion of the detailed risk assessment, if it is determined that there
        - has been an eligible data breach, see clause 11a.
        - has not been an eligible data breach, see clause 11b.

Notifiable data breaches

(12) On receipt of the data breach assessment report, the Data Breach Response Team will assess and determine if it is a notifiable data breach.

(13) If it is determined that it is a notifiable data breach, the Data Breach Response Team will:

a. complete a list of individuals impacted
b. consider if there is any additional information required to support the:
    i. data custodian
    ii. impacted individuals
    iii. completion of the Notifiable Data Breach Statement - form
c. prepare a Notifiable Data Breach Statement - form
d. submit the Notifiable Data Breach Statement - form to the University's privacy officer (who will approve and

submit to the OAIC, along with any approved additional information)

e. notify and advise impacted individuals, relevant University areas and the Office of the Vice-Chancellor that:
    i. possible vulnerabilities have been identified
    ii. a Notifiable Data Breach Statement - form has been lodged
f. advise remedial actions to be undertaken by relevant stakeholders
g. monitor the delivery of remedial actions
h. capture and report on success of remedial actions undertaken by relevant stakeholders.

(14) If it is determined that it is not a notifiable data breach, the Data Breach Response Team will:

a. consider how the data breach occurred
b. recommend enhanced personal information security measures
c. communicate and provide recommendations to the data custodian and relevant stakeholders.

Responsibilities

(15) Charles Sturt University staff are responsible for:

a. reporting via the IT Service Desk as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the University
b. protecting personal information held by the University against unauthorised disclosure.

(16) Charles Sturt University students are responsible for:

a. reporting via SX Service Centre as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the Universitymaintaining appropriate data protection of their personal data.

(17) IT Service Desk is responsible for:

a. registering reported incidents
b. providing specialised advice (where possible) to the individual reporting the incident on options for preventing further damage
c. escalating the incident within the IT Service Management Platform to ICT Security Team.

(18) SX Service Centre is responsible for:

a. registering reported incidents
b. providing specialised advice (where possible) to the individual reporting the incident on options for preventing further damage
c. escalating the incident within the IT Service Management Platform to ICT Security Team.

(19) ICT Security Team is responsible for:

a. assessing assigned security breaches
b. reporting breaches to the Data Breach Response Team.

(20) Data Breach Response Team are responsible for:

a. actioning the data breach response process within specified time constraints

b. maintaining adequate documentation of suspected data breaches reported and steps taken to deliver on compliance and University reporting requirements
c. preparing and submitting to the privacy officer the Notifiable Data Breach Statement - form where applicable
d. checking personal data breach incidents to see if it also fits the critical incident classification
e. notifying the Crisis Management Team of any suspected or identified critical incident.

(21) The privacy officer is responsible for:

a. overseeing the University's compliance to Notifiable Data Breaches scheme
b. managing the University's data breach response plan
c. chairing the Data Breach Response Team meetings
d. approving the prepared Notifiable Data Breach Statement - form
e. lodging the Notifiable Data Breach Statement - form to OAIC
f. reporting to the Vice-Chancellor on notifiable data breach compliance and OAIC notifications
g. approving any additional information about a University data breach that is to be provided to impacted individuals or other third parties. This could be in addition, or separate to a Notifiable Data Breach Statement - form.

(22) Chief Information and Digital Officer is responsible for:

a. contributing as a member of the Data Breach Response Team
b. supporting the availability of technical expertise to undertake data breach response and remedial actions.

(23) Data Security and Governance Committee is responsible for:

a. promoting the adoption of information management and ICT security controls to ensure integrity, availability and confidentiality of personal information
b. providing guidance on improvements to protect personal information from unauthorised disclosure.

(24) Application, data and information custodians are, for the personal information and data within their area of responsibility, responsible for:

a. reporting via the IT Service Desk as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the University
b. actively managing and maintaining protection against unauthorised disclosure. This includes aspects such as:
    i. capture, use, movement, storage and retention of information
    ii. access controls for both electronic and physical records
    iii. staff training (including manual handling)
    iv. monitoring for unauthorised disclosure.

(25) The Crisis Management Team and Critical Incident Management Team are responsible for notifying the Data Breach Response Team of any suspected or identified personal data breaches.

Section 4 - Guidelines

(26) Nil.

Section 5 - Glossary

(27) This procedure uses terms defined in the Information Technology Policy, as well as the following:

a. Application, data and information custodians – means the nominated staff overseeing the management of a specified application, data or information set with regards to ensuring availability, integrity, and protection according to relevant University business requirements, policy and legislative compliance.
b. Data breach response plan – means the University's plan that sets out the components, roles and responsibilities for managing the University's appropriate response to a data breach.
c. Data breach response process – means the actions to be taken in the case of a suspected or identified data breach. Facilitates a swift response and ensures any legal obligations are met following a data breach.
d. Data Security and Governance Committee – a subcommittee of the Technology Governance Committee.
e. Eligible data breach – means:
    i. unauthorised access to or disclosure of, or loss of, personal information held by the University, and
    ii. this is likely to result in serious harm to one or more individuals, and
    iii. the organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.
f. Information security - encompasses:
    i. ICT security policies
    ii. organisation of information security
    iii. ICT asset management
    iv. information security compliance obligations
    v. information security components of human resources management
    vi. ICT communications and operations management
    vii. information security components of business continuity management
    viii. ICT services access control
    ix. ICT security incident management
    x. ICT systems acquisition, development and maintenance
    xi. ICT asset physical and environmental security.
g. ICT Security Team – comprised of specialised Division of Information Technology resources who are responsible for the confidentiality, integrity and availability of the University's information assets.
h. Notifiable data breach – means a personal data breach that is determined as having a real risk of serious harm to the affected individual(s). A notifiable data breach requires at a minimum, formal notification to the OAIC and affected individuals.
i. Notifiable Data Breaches scheme – requires regulated entities to notify impacted individuals and the OAIC about eligible data breaches.
j. Personal data breach – means personal information or data held by the University is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Data breaches can be accidental or intentional in nature.
k. Personal information – as defined in the Privacy Management Plan.
l. Preliminary data breach assessment – means the initial assessment completed to determine quickly if there is a high level of risk of serious harm to affected individuals given the nature and scope of the personal data breach.
m. Privacy officer – means the University officer, as stated in the Privacy Management Plan, who oversees the maintenance of the University's Privacy Management Plan and provides advice and support to the University in meeting privacy legislation obligations.
n. Serious harm – means serious harm to an individual and may include:

i. identity theft
ii. financial loss
iii. threat to physical safety
iv. threat to emotional wellbeing
v. loss of business or employment opportunities
vi. humiliation
vii. damage to reputation
viii. bullying, or
ix. marginalisation.

o. Unauthorised access – means personal information that an organisation holds is accessed by someone who is not permitted to have access.
p. Unauthorised disclosure – means an organisation has made personal information accessible or visible to others outside the organisation, and released that information from its effective control in a way that is not permitted by the Privacy Act 1988.

Status and Details

Status	Current
Effective Date	1st August 2022
Review Date	1st August 2025
Approval Authority	Chief Operating Officer
Approval Date	30th July 2022
Expiry Date	Not Applicable
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Vanessa Salway Manager, Policy and Records
Enquiries Contact	Division of Information Technology +61 2 63386260