

Schedule 8

Caldicott Principles

Part A Summary of the 6 Caldicott General Principles

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personally-identifiable information within or from an organisation should be clearly defined and scrutinised with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary

Personally identifiable information items should not be used unless there is no alternative.

Principle 3: Use the minimum necessary personally identifiable information

Where use of personally identifiable information is considered to be essential each individual item of information should be justified with the aim of reducing identifiability.

Principle 4: Access to personally-identifiable information should be on a strict need to know basis

Only those individuals who need access to personally identifiable information should have access to it and they should only have access to the information items that they need to see.

Principle 5: Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling personally identifiable information – both practitioner and non-practitioner staff – are aware of their responsibilities and obligations to respect an individual's confidentiality.

Principle 6: Understand and comply with the law

Every use of personally-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Part B Information Governance

Information Security Requirements

The Provider shall apply appropriate technical and organisational measures to adequately secure the Council's personal data during processing, storage and transfer. These measures must fulfil the Council's legal obligation to comply with data protection principle 7 (Information Security) of the Data Protection Act 1998. In furtherance of this the Provider shall indemnify the council for loss or damages caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

1. Information security policy shall be in place, approved by management, communicated to employees and sub-contractors and available for inspection.

2. Information security responsibilities shall be assigned to one or more competent individuals.
3. The Provider shall notify the Council's Information Security Officer of any incidents of breach or loss of the Council's data as soon as reasonably practical and in any case no later than 72 hours after becoming aware of an incident.
4. Background checks are undertaken and employment contracts and sub-contracts include appropriate terms, conditions and disciplinary sanctions to minimise risks to the confidentiality and integrity of Council data.
5. Business continuity / Disaster recovery plan(s) shall be in place (or will be at service commencement) to address unavailability event(s) or incident(s).
6. The Provider shall comply with any reasonable request for change to its service that is required to ensure the council's continued compliance with the Public Service Network (PSN) Code of Connection (CoCo). This applies a baseline security standard to which all PSN connected parties are required to adhere.
7. Appropriate controls shall be in place to protect Council data from malicious code or cyber-attacks.
8. Assets storing or processing Council data shall be appropriately protected against physical tampering, loss, damage or seizure.
9. Audit logs shall record relevant user activity, exceptions and information security events such that incidents or suspicious activity can be adequately investigated and attributed.
10. Measures shall be in place to identify and treat technical vulnerabilities (e.g. patching and updates) in a timely and appropriate manner.
11. Controls shall be in place to ensure other customers of your service are unable to access the Council's data or threaten its service (either maliciously or as a result of their own service being compromised).
12. Controls shall be in place to minimise the risk of portable or online storage devices and/or services being used by the Provider's employees or sub-contractor for the unauthorised copying or removal of Council data.
13. Provider employee and sub-contractor accounts shall be revoked in a timely manner in the event of termination of employment or change of role.
14. System Administrator accounts shall not be shared and shall only be allocated to named individuals who are accountable for their actions.
15. User accounts shall be created or revoked in a timely manner in response to requests from the Council or on your termination of employee agent or sub-contractor.
16. Secure Remote Access shall be available as an option.

17. The Provider shall agree to supply to the Council personal information relating to employees, agents and sub-Provider s with access to Council information for the purpose of completing background checks in accordance with our obligations under PSN CoCo.
18. The Provider's employees, agents and sub-Provider s shall complete specialist data protection training designed for those who handle data at this classification within the first six months of service commencement.
19. Networks shall be managed and controlled in a way that is appropriate to this classification of data.
20. Measures shall be in place to enable the detection and attribution of misuse or unauthorised activity.

Cloud Security Requirements

The Provider shall comply with ALL of the following requirements for any part of their service that uses web hosting, web applications or cloud services:

Requirements for OFFICIAL or Personal Data
1. User access via browsers shall be configured to use HTTPS security and using Transport Layer Security version 1.2 as a minimum (TLS1.2).
2. Cryptography certificates shall be issued by a current member of the Certificate Authority Security Council (CASC).
3. A Penetration Test of web facing services shall be performed by a CREST registered tester and high risk issues remediated before service commencement.
4. Appropriate controls shall be in place to protect Council data from malicious code or cyber-attacks.
5. Appropriate technical controls shall be in place to protect Council data in the event of the theft, loss or transfer of ownership of a privately owned device previously used to access the service.
6. Two-factor authentication (2FA) shall available as an option.

Requirements for OFFICIAL-SENSITIVE or Sensitive Personal Data¹ or CONFIDENTIAL INFORMATION²
1. Extended Validation (EV or Green Bar) cryptography certificates shall be provided (or will be at service commencement) by a current member of the Certificate Authority Security Council (CASC).
2. The Provider shall supply to the Council such personal information relating to employees with access to Council data in this classification as is necessary for background checks to be initiated as required for the council to comply with its PSN Code of Connection.
3. The Provider's employees will complete specialist data protection training designed for those who handle data at this classification within the first six months of service commencement.
4. Networks shall (or will at service commencement) be managed and controlled in a way that is appropriate to this classification of data.
5. Web applications and/or Cloud services shall (or will be prior to service commencement) be penetration tested by a CREST approved Provider at annual intervals. Test results shall be made available to the contracting Council on request.
6. Two-factor authentication (2FA) shall be provided.

¹ 'Sensitive Personal Data' means Data Protection Act definition relating to an individual's health, race, ethnicity, political or religious beliefs.

² 'Confidential Information' relates to an individual's health or ADULT social care (Health and Social Care Act 2012).