information management & security

Gloucestershire COUNTY COUNCIL

Information Security & Handling Standards for Contractors Policy

Introduction

Gloucestershire County Council's Cyber & Information Management (Procurement) Policy sets out the standards and best practice that the Council requires its Providers (including sub-Providers) to have in place as part of the service they will provide. In particular the Provider should have appropriate and relevant technical, physical and organisational measures (Protective Measures) in place to protect Council data.

In addition to those standards, Providers that process Council owned personal data are also required to observe and comply with the procedures and standards set out in this document.

Contents

Definitions

- **Personal data** – Data about a natural, living individual, who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. Pseudonymised data (i.e. personal reference numbers or unique identifiers) can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

- **Data subject** – The natural, living individual of who personal data is about or relates to.

- **Special category data** – Personal data about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

- **The Council** – Gloucestershire County Council.

- **The Provider** – the third party providing a service or supplying the Council with a service as part of a contract or other agreement.

1. Privacy Management

- The Provider must take appropriate steps to safeguard the privacy of data subjects and only process personal data on behalf of the Council in line with the Data Processing Schedule.
- The Provider must comply with the relevant privacy notice for the service.
- Where the Provider proposes to create a new or amend an existing system/process affecting the processing of personal data, the proposal must be referred to the relevant commissioner/contract manager who will liaise with the Council's Information Management Service on whether a Data Protection Impact Assessment needs to be reviewed or undertaken.

2. Information Security Incident Process

- Any Personal Data Breach, Data Loss Event or breach of the Data Processing Schedule of the Contract and/or this policy (collectively known as an information security incident) must be investigated and may result in contractual action.
- The Provider must have processes in place to capture and manage information security incidents.
- Where regular performance reporting is required by the Council, the Provider must provide Information Security Incident statistical data. Detailed Information Security Incident evidence must be supplied on demand.
- The Provider must report all information security incidents immediately to the relevant the Council contract manager/commissioner and the Information Management Service for formal notification as soon as they are identified and must update the Council on the investigation progress and final resolution as directed.
    - **If using a secure email**, send details to:
        - informationsecurity@gloucestershire.gov.uk
    - **If using unsecure email**, in the first instance, email the above contact to notify the Council of the breach, without any personal data or commercially sensitive information. Following this, the Council will respond via secure email for further detail, as required.
- Criminal incidents (such as theft of equipment that contains the Council data) must also be reported to the police. The Provider must pass on any reference number provided by the police to the Council.

3. Data Subject Rights

- The Provider shall assist the Council in safeguarding the relevant applicable legal rights of the Data Subject as identified in the privacy notice for the service being delivered. These rights are;
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erasure (Right to be forgotten)
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - The right to object to Direct Marketing
    - Rights related to automated decision making and profiling
- If the Provider receives a Data Subject Right Request they are to immediately notify the Council's Information Management Service.
    - **If using secure email** send details to:

        - foi@gloucestershire.gov.uk
    - **If using unsecure email**, in the first instance, email the above contact to notify the Council of request, without any personal data or commercially sensitive information. Following this, the Council will respond via secure email for further detail as required.
- If the Council contacts the Provider with a Data Subject Right Request, the Provider shall provide action on the request within 10 working days of receipt of instruction by the Council, unless an extension is agreed with the Council.

4. Security Classification

- Providers must comply with Government Security Classifications Policy when processing information on behalf of the Council.
- All information processed by or on behalf of the Council falls within the category of 'OFFICIAL', with some data falling within the sub section 'OFFICIAL-SENSITIVE', as defined by the UK Government.
- 'OFFICIAL-SENSITIVE' information will usually be marked in this way so that individuals and organisations other than the Council understand that there is need for further controls to be in place, particularly in respect of sharing.

5. Staff Vetting and Training

- As part of the employment process, all Provider and sub-Provider staff with access to Council data including those involved in the administration, hosting, support and / or development of software applications processing Council data shall be adequately vetted and trained.
- Vetting must include:
    - employee disclosure of any convictions which are not yet spent;
    - verification of identity, nationality and immigration status, and;
    - three years of references including explanation of employment gaps.
- The Provider must ensure staff are aware of their responsibilities regarding information security and policy compliance. A staff disciplinary process must be in place to address any compromises to Council information assets.

6. Policies

- The provider shall maintain and review policies that cover the following:
    - Data Protection
    - Information Security
    - Records Management
    - Information Sharing
    - Removable media
- The provider shall provide copies of the policies that cover these topics to the council upon request.

7. Information Management

7.1. Accessibility

- The Provider must ensure that the Council data held on its systems is maintained in such a way that those who have the rights to access can:
    - Do so promptly;
    - Easily identify and locate information
    - Easily establish the most current and complete version
    - Understand who they may share it with and under what circumstances
    - Easily establish audit trails of services delivered and related authorisations, for use in the Council performance monitoring and internal or external auditing.

7.2. Data Quality

The Provider must provide quality data processes to support effective service delivery and decision making. Quality data has the following characteristics:

- **Accurate:** It must provide a true account of what it is intended to represent to enable informed decisions to be made. Maintaining the accuracy of Personal Data is a requirement of Data Protection law.
- **Valid:** Data must appropriately reflect what it is intended to measure or report
- **Reliable:** Data must be consistently calculated, recorded, analysed and reported over time in a way that provides a meaningful reflection of the situation.
- **Timely:** Data must be available frequently and captured promptly enough to be of value
- **Relevant:** Data must be defined/ selected, collected, recorded and analysed with the intended use and audience in mind so that it is fit for purpose and adds value.
- **Complete:** Data must be complete and comprehensive to ensure it provides a full picture of a current situation, and caveated where it is incomplete.

The Provider must support regular reviews, sample auditing and provide feedback to achieve and maintain an acceptable standard of data quality.

7.3. Retention and destruction

- Council data must be retained in line with the Council's Corporate Retention Schedule and destroyed securely as set out in the Data Processing Schedule of the contract.
- Where the Provider destroys data, this activity must be evidenced by recording the criteria for destruction, approval, date and method of the destruction activity and a certification of completion.
- Where the Provider has the authority to dispose of the Council data in accordance with the Council Corporate Retention Schedule or by virtue of

any additional agreement, the data must be disposed of by methods appropriate to its security classification.

- Destruction processes must ensure that the data is kept secure from disclosure to unauthorised persons until and during destruction, and that the data cannot be reconstituted after the destruction process.

8. Asset Management

- A register must be maintained of the physical hardware items (assets) which the Provider uses to access the Council data
- Paper records must be stored in lockable equipment or dedicated rooms with access to keys or codes managed;
- Paper filing systems must be well maintained, using clear, logical and consistent referencing and kept in good condition to support identification and retrieval
- When paper records are being transported they must not be left unattended, must be kept out of sight when not being used, and (where available) stored in secure transportation such as a code-lock case.
- Where paper records contain OFFICIAL-SENSITIVE Council data, removing them from storage must be a recorded activity.
- The Provider must maintain a current and accurate knowledge of the Council data it holds in all formats, on what systems it resides and the physical locations in which those systems are stored.
- Internal ownership must be established with owners aware of their responsibilities under these requirements.

9. IT and information security

9.1. Staff training

- All Provider staff must be adequately trained according to the role they are to perform when using Council data.
- All Provider staff must undertake information security training prior to being given access to Council data. This training must be completed at least every two years.
- The Provider must be able to demonstrate to the Council that their staff have completed information security training upon request.

9.2. Access Controls

- The Provider must have access control in place for granting and revoking access to information and systems.
- The Provider's access control procedures must include clear responsibility for:
    - Checking that proposed access is appropriate to the business purpose,
    - Authorising access, and

- Promptly removing or blocking access for users who have changed roles or left the organisation.

9.3. Equipment Security

Devices accessing Council data (such as desktops, laptops, tablets, mobile phones etc.):

- Users must not access Council data on devices that do not have relevant protective measures in place.
- Equipment must be switched off or 'locked' after an appropriate period of inactivity and require a password to re-access.
- When stored in office space, laptops must be secured with lock devices or in lockable storage to prevent theft.
- When devices accessing Council data are used in users' homes, they must be protected from use by any unauthorised persons and must be stored out of sight when not in use to prevent theft.
- When laptops are being transported they must not be left unattended. They must be kept out of sight when not being used.
- Any individual for whom the Provider is responsible (and who accesses Council data) must return devices to the Provider when their role requiring access to the Council data ends, or their role no longer entitles them to such equipment
- Devices accessing Council data should not be taken outside of the UK or European Economic Area (EEA) unless
  - a) there is a strong business need approved by the Provider's governance processes and by Council; and
  - b) there are sufficient security controls in place on the device to allow its use without exposing Council data to malicious activity or unauthorised disclosure.
- Users must report lost or stolen equipment to the Provider immediately and where any Council data is at risk the loss must be handled as an Information Security Incident

9.4. Removable media

- Removable media refers to USB drives, CDs, DVDs, secure digital cards and devices which permit the storage of data on memory cards, but also refers to hard-copy such as paper files.
- Removable media should only be used where there is a clear business need.
- Where the Provider allows for the use of removable media, the Provider must encrypt to an appropriate level any device storing digital Council data that would cause damage or distress to individuals, or reputational damage to the Provider or the Council if it were lost or stolen.

- The Provider must ensure that the level of security applied to office-located devices is applied to Council data on removable media being used away from the office.
- Personal data must only be held on removable digital media for transfer purposes and must be securely deleted once copied to its formal storage location.
- The Provider must maintain a removable media policy for the storage of information that:
    - Controls access to, and the use of removal media.
    - Limits the type of media that can be used,
    - Defines user permissions, and the information types that can be stored.
    - Ensures that all clients and hosts automatically scan removable media for malware before first use, and any subsequent data transfer takes place
- Where removable media is to be reused or destroyed, appropriate steps should be taken to ensure that previously stored information will not be accessible.

9.5. Encryption – data at rest

- The Provider must not store and personal or sensitive Council data on any user device (including mobile devices, tablets, laptops or computers) unless it is encrypted.
- If a device is not already supplied with encryption then the Provider should use an encryption product such as Bitlocker or Becrypt.
- Adequate protection must be in place for the handling and storage of associated cryptographic items (e.g. encryption keys, SSL certificates etc).

9.6. Passwords

- All passwords must be managed securely. Strong passwords must be used for any system that holds Council personal data. Strong passwords must be of 8 characters or more, with the use of mixed case alphanumerics with other symbols and not be based on a dictionary word.

9.7. Back ups and business continuity

- The Provider must take regular backups of Council data they hold, and make sure these backups are recent and can be restored in a timely manner so that there is minimal impact on service provision.
- Back up data must be;
    - Kept separately from and not permanently connected to the device or system holding the original copy.
    - Only accessible by appropriate staff with a responsibility for IT.
    - Held securely (e.g. strongly encrypted at rest).

- Business continuity and disaster recovery plans must be in place and tested to ensure its ongoing effectiveness.

9.8. Testing

- Council data must not be stored on any test environment without prior consent from Council and unless the Provider ensures that the test environment exhibits identical security contracts as the production environment.
- Where the Council provides consent, then test facilities should exhibit identical security controls to those being used in the production environment and only as defined and agreed by Council.

9.9. Patching and updates

- All software used to process Council data must be kept patched and updated in a timely manner. A patching / firmware update process must apply to all components, including but not limited to servers, workstations, network devices, firewalls, storage area networks and appliances.
- The following are recommended timeframes for applying and verifying patches based on the outcome of risk assessments for security vulnerabilities:
  - extreme risk: within 48 hours of a patch being released
  - high risk: within two weeks of a patch being released
  - moderate or low risk: within one month of a patch being released.
- Additionally, Independent assessments (IT Health Checks) must be conducted on a regular basis to confirm the effectiveness of patching.

9.10. Secure data transfer during service provision

- There may be a requirement to transfer data between Council and the Provider during the development, setup and ongoing management of the service. Any data transfer between Provider and Council must be done using secure transfer mechanisms
- Physical and removable media must only be used to transport information between Council and the Provider when the transfer cannot be achieved using a secure network connection. When removable media is used to exchange personal and/or sensitive information between Council and the Provider then it must be encrypted at all times.

9.11. Encryption – data in transit

- All personal or sensitive data transmitted over public networks must be encrypted in transit. This includes staff working remotely and accessing internal systems that store confidential data and staff supporting and administering the system.
- Electronic messages (including email and electronic messaging) must not contain personal data unless authorised and encrypted prior to sending.

9.12. Email

- The Provider must ensure that employees are aware of the importance of correctly addressing emails (as with hard-copy mail), to reduce instances of loss of Council data or it being received by an incorrect recipient.
- Where the Provider needs to send Official-Sensitive Council data by email (or post), the Provider must ensure that employees have been authorised to do so and follow the security classification requirements.
- Where secure email facilities are not available, emails must be sent with the Official- Sensitive Council data in a password protected attachment, with the recipient informed of the password via an alternative method to email.
- Where the Provider's employees send Council data to the incorrect recipient, the Provider must manage this as an Information Security Incident and ensure the data is recovered. If the data is personal this must be reported to Council in line with the Information Security Incident Process in order to consider further actions in regards to the data subject and supervisory authority.

9.13. Secure Email

- Where the Provider has access to secure government systems such as PSN, CJSM etc and the recipient is able to receive securely, then these facilities must always be used to send Council Official-Sensitive and personal data.
- Where the Provider has access to secure email tools then these facilities must always be used to send Official-Sensitive Council data.

10. Physical Security

10.1. Use of Council Premises:

- Where the Provider is/are based in or utilise Council's premises, the Provider must ensure that they comply with Council ID Cards and Building Security Policy (See section 10.3).
- The Provider must supply data on request of those employees who it approves to hold Council ID cards. Such data must be sufficient to identify individual employees to manage their card entitlement.
- The Provider must advise Council immediately of any individual leaving their organisation so that access to Council premises can be terminated.

10.2. Use of Non-Council Premises:

- The Provider must ensure that premises (and dedicated areas where Council data is stored within premises including any Cloud Storage) are protected against unauthorised entry and theft of or damage to Council data.

- Access to building entry keys and keys which secure rooms or storage equipment must be controlled and custody recorded.
- The Provider must regularly change access codes and change relevant codes immediately when an individual's right of access expires.

10.3. Council ID Cards and Building Security Policy:

- You must not allow anyone to follow you through a security door (tailgating) without clearly displaying a valid ID Card.
- You must carry your Council ID Card or Visitor pass and display it at all times when in Council buildings, or to prove to a member of the public or staff of another organisation that you are representing Council on official business. Otherwise, when outside of Council premises you should keep your pass hidden to ensure personal security.
- You must not share your Council ID Card with anyone, or share door codes or keys with unauthorised people.
- If you find a lost Council ID Card, you must hand it in to the nearest reception or security office.
- If you lose your pass or it is stolen, you must report it via BSC or custodians.
- All leavers must hand their pass to their line-manager as part of the leavers' process.
- You must supervise all visitors that you allow into a secure work area at all times until they leave. Unless on the Property Services' Framework of Providers.
- You must ensure door codes and security alarms are changed regularly, where in use.
- All employees must ensure offices are secure if they are the last person to leave at the end of the working day.

11. Collaboration Sites

Where the Provider is granted access to sites hosted by the Council which allow the sharing of and collaboration on information of mutual interest, the Provider must ensure that:

- There is a register maintained of employees who have access to sites, and that the access is at all times necessary and therefore valid and available for auditing by Council.
- Where employees leave the organisation, or when they change to a role which no longer requires access or when access credentials have been compromised, the Provider must inform the relevant Council SharePoint Site Manager to allow accounts and permissions to be managed accordingly

- Those with rights to add or edit documents must comply with the Council Site Owner's requirements over assigning document metadata, titling conventions and correct document library storage
- Copies of documents containing Council data available on the sites are not stored outside of the site or shared/ disclosed beyond the permissions group of the site without the permission of the Site Owner.
- Where a site is accessible by a number of Providers, Providers and Partners, any information which a Provider does not wish to be available to anyone other than Council and its own employees must be stored in a document library for the appropriate audience, provided by Council.
- Its employees are aware that all information on the site is accessible to Council and is information held by Council for the purposes of the Freedom of Information Act (2000). Wherever possible the Provider will be offered the opportunity to provide prejudice and public interest representations for the Council to consider, prior to disclosure.
- Where the Provider is a Public Authority under Schedule 1 of the Freedom of Information Act (2000), its employees must be aware that disclosure of any Council data stored on a site in response to requests for information must be referred to Council for clarification on whether the data is held for the purposes of the Act, and if so, for consideration of valid exemptions.

12. Version Control

Author	Nick Holland, Senior Information Governance Adviser
Owner	Jenny Grodzicka, Head of the Information Management Service (DPO)
Created Date	1 January 2020
Review Date	1 January 2021
Version	1