

**CCP085**

**Security at Chesterfield Library**

**Appendix H**

**Supplier Information Security**

Contents

[1. Background 3](#_Toc56773294)

[2. Instructions 3](#_Toc56773295)

[3. Controls – 5% Weighting 4](#_Toc56773296)

# Background

Derbyshire County Council provides essential services and business functions which rely on IT solutions and applications contracted by third party suppliers, which may be primary or sub-contractors. The Council relies on the integrity and accuracy of its information in order to carry out its business and obligations to the public. These include meeting its data protection obligations under the General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA) which places statutory obligations on data controllers and processors who are involved in the processing of personal data. The Council has itself achieved certification to the ISO27001:2013 standard and has established an Information Security Management System (ISMS) in accordance with the requirements of ISO27001 and ISO27002 code of practice for information security controls.

This document sets out the minimum supplier information security and data protection controls for contracts, service arrangements, grant awards and partnership agreements that involve IT solutions or provision of services which require access to, or the processing of, personal data for the delivery and/or support of Council services and business functions. The information security and data protection requirements that potential suppliers are asked to meet as part of the procurement process reflect the nature of the service and the sensitivity, volume and risk associated with the information held. The controls aim to protect the Council’s interests by providing a flexible approach to managing information security risks during contractual arrangements.

As the Contract involves the procurement of an IT solution or a service which, in part, is reliant upon an IT solution to process personal data, the procurement will be assessed against the current data protection regulations to determine the associated level of perceived risk to the Council.

The ‘type of personal data’ will lead to one of three classifications; “Restricted Data, Controlled Data or Public Data” in accordance with the Council’s Supplier Information Security Policy (available [here](https://www.derbyshire.gov.uk/working_for_us/data/away_from_your_desk/working_with_the_public/default.asp)). This data has been classified as **Restricted**.

# Instructions

Tenderers are required to select the relevant response box (**Yes** or **No**) for each control in the tables below; thereby ‘ticking’ to confirm whether their organisation or Solution (as appropriate) is compliant or not.

Where the Contract is for a Solution, which is to be hosted ‘on premise’ by the Council, Tenderers should respond to the controls on the basis that third parties have access to the Data (including suppliers, contractors, sub-contractors and employees) e.g. during data migration or whilst providing support and maintenance services.

If not compliant, only partially compliant or not applicable, Tenderers shall select the No response and complete the Comments column to indicate the degree of non-compliance, the date(s) within which they will become compliant and an indicative action plan to achieve full compliance or a full explanation of why the control is not applicable; **failure to do so will affect the scores allocated.**

Responses to each control will be evaluated and scored in accordance with the Guidance Notes and Instructions to Tender.

# Controls – 5% Weighting

**Restricted Data**

**Section One – Independent Certification**

Council contracts for major IT solutions and contracts that involve the processing and/ or retention of high volumes of personal data, and the processing of special categories of personal data, as defined within the Data Protection Impact Assessment (DPIA), require to the supplier being accredited to the Cyber Essentials Plus certification (or equivalent). Suppliers will be expected to be compliant with this requirement either prior to the contract award date or during the initial stages of the contract start date.

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** | **Expected Control – Cyber Essentials Plus**  | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 1.1 | Where deemed necessary, the supplier holds a current ‘Cyber Essentials Plus’ certification (or equivalent) | Yes [ ]  | No [ ]  |  |
| 1.2 | The supplier holds a current ‘Cyber Essentials’ certification (or equivalent)  | NOT APPLICABLE |

**Section Two – Core Data Protection and Information Security Questions for all Suppliers**

The table below, sets out the minimum data protection and information security controls for IT solutions or services where there is a requirement for the storing, handling, processing or retention of the Council’s personal data by third parties (including suppliers, contractors, sub-contractors and employees).

|  |  |  |  |
| --- | --- | --- | --- |
| **2.** |  **Expected Control – Staff Related** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.1 | Do you have written contracts of employment for your staff, which include reference to your information security policies and procedures? | Yes [ ]  | No [ ]  |  |
| 2.2 | Do you provide all of your staff, volunteers and agency workers with a formal induction that includes information security and data protection guidance? | Yes [ ]  | No [ ]  |  |
| 2.3 | Are your staff, volunteers and agency workers provided with annual training/ updates on information security and data protection? | Yes [ ]  | No [ ]  |  |
| **Ref.** |  **Expected Control – Policies** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.4 | Do you have information security policies in place which your staff, volunteers and agency workers are required to comply with? | Yes [ ]  | No [ ]  |  |
| 2.5 | Do you have a Password Policy for your staff, volunteers and agency workers which requires all individuals to have a unique account and password? | Yes [ ]  | No [ ]  |  |
| 2.6 | Does your Password Policy require your staff, volunteers and agency workers to have a password that is at least twelve characters in length, include complexity requirements and are periodically changed? | Yes [ ]  | No [ ]  |  |
| 2.7 | Are staff, volunteers and agency workers trained not to disclose their password to anyone? | Yes [ ]  | No [ ]  |  |
| 2.8 | Do you have a Bring Your Own Device Policy which outlines your requirements in terms of staff, volunteers and agency workers using personal equipment at work? | Yes [ ]  | No [ ]  |  |
| 2.9 | Are staff, volunteers and agency workers restricted from using personal equipment (i.e. laptops, phones, USB devices) for business activities? | Yes [ ]  | No [ ]  |  |
| 2.10 | Do you restrict your staff, volunteers and agency workers from using personal email accounts or personal cloud-based storage as part of normal business activities? | Yes [ ]  | No [ ]  |  |
| 2.11 | Do you have a Homeworking Policy for all staff, volunteers and agency workers? | Yes [ ]  | No [ ]  |  |
| 2.12 | Have you undertaken a risk assessment in terms of information security and Homeworking arrangements? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – User Permissions** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.13 | Do you ensure that staff, volunteers and agency workers are only provided with the access to information, files and documents required to undertake their role? | Yes [ ]  | No [ ]  |  |
| 2.14 | Do you periodically review (at least every six months) staff, volunteers and agency workers access permissions to ensure they reflect their current roles?  | Yes [ ]  | No [ ]  |  |
| 2.15 | Do you have a process in place to ensure that staff, volunteers and agency workers access to your computers and IT network is removed promptly when leaving and that all assets including keys, computers and documents are returned? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Network**  | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.16 | Do you have a firewall (or similar network device) installed on the boundary of your internal network? | Yes [ ]  | No [ ]  |  |
| 2.17 | Do you restrict the ability to install software on your IT equipment (i.e. laptops and PCs) to senior managers or system administrators? | Yes [ ]  | No [ ]  |  |
| 2.18 | Is anti-virus and malware software installed and regularly updated on all of your IT equipment (i.e. servers, computers and laptops)? | Yes [ ]  | No [ ]  |  |
| 2.19 | Are all your computers and devices hard drives protected by encryption (e.g. Windows Bitlocker)?  | Yes [ ]  | No [ ]  |  |
| 2.20 | Do you ensure that where information is transmitted over the Internet the connections are secured by encryption? (e.g. HTTPS/ TLS v1.2 as a minimum) | Yes [ ]  | No [ ]  |  |
| 2.21 | Do you have the ability to send and receive secure, encrypted emails when communicating/exchanging restricted or confidential data with the Council? | Yes [ ]  | No [ ]  |  |
| 2.22 | Do you undertake an annual vulnerability scan of your internal network to highlight potential security issues? | Yes [ ]  | No [ ]  |  |
| 2.23 | Do you undertake an annual vulnerability scan of your external network to highlight potential security issues? | Yes [ ]  | No [ ]  |  |
| 2.24 | Do you retain audit logs from your Internet, server and IT network usage for at least 30 days? | Yes [ ]  | No [ ]  |  |
| 2.25 | Do you restrict staff from sending confidential or personal data via SMS, text or instant messaging services?  | Yes [ ]  | No [ ]  |  |
| 2.26 | Do you ensure that staff mobile devices including phones and iPads holding confidential or personal data are secured by the use of a ‘PIN’ | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Patch Management** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.27 | Do you apply security patches (e.g. Microsoft Windows updates) to all software running on your computers and network devices? | Yes [ ]  | No [ ]  |  |
| 2.28 | Has out of date software been removed from your computers and network devices (e.g. Windows XP or Windows 7)? | Yes [ ]  | No [ ]  |  |
| 2.29 | Do you apply vendor updates and application updates to your smart phones? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Business Continuity** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.30 | Do you have a Disaster Recovery and Business Continuity Plan in place for your organisation? | Yes [ ]  | No [ ]  |  |
| 2.31 | Do you periodically test (at least annually) your Disaster Recovery and Business Continuity Plan? | Yes [ ]  | No [ ]  |  |
| 2.32 | Do you regularly take backups of your IT systems and its data? | Yes [ ]  | No [ ]  |  |
| 2.33 | Are your backups protected by encryption and held in a separate location to the main data? | Yes [ ]  | No [ ]  |  |
| 2.34 | Do you have a process in place to ensure that information security incidents are identified promptly and notified to the Council (where applicable)? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Data Retention and Disposal** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.35 | Do you have a Data Retention Policy which includes the automatic deletion (where appropriate) of information where the retention period has been exceeded? | Yes [ ]  | No [ ]  |  |
| 2.36 | Do you have a procedure in place to manage the retention period for email records and other records including Microsoft Word and Excel records, PDF documents and photos? | Yes [ ]  | No [ ]  |  |
| 2.37 | Do you have a process in place for the secure disposal of old IT equipment including hard drives, which is supported by certificates of disposal?  | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Manual Records** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.38 | Are all paper records containing the confidential or personal data held securely on-site or as part of off-site storage facilities? | Yes [ ]  | No [ ]  |  |
| 2.39 | Do you have a process in place for the secure disposal of paper documents and sensitive information, which is supported by an audit trail? | Yes [ ]  | No [ ]  |  |
| 2.40 | When transporting confidential or personal data by vehicle are staff aware of the requirement that all records and IT equipment must be held securely when left unattended? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Legal Compliance** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.41 | Do you have procedures in place to monitor compliance with the Data Protection Act 2018 and General Data Protection Regulation? | Yes [ ]  | No [ ]  |  |
| 2.42 | Do you have procedures in place to monitor compliance with the Computer Misuse Act (1990)? | Yes [ ]  | No [ ]  |  |
| 2.43 | Do you have procedures in place to monitor compliance with the Privacy and Electronic Communications Regulations (2019)? | Yes [ ]  | No [ ]  |  |
| **Ref.** | **Expected Control – Third Parties** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 2.44 | Do you have contracts in place with all of your third party suppliers i.e. IT support or data hosting company? | Yes [ ]  | No [ ]  |  |
| 2.45 | Have you undertaken appropriate due diligence checks on third party suppliers that have access to personal data i.e. IT support and CRM system providers? | Yes [ ]  | No [ ]  |  |

**Section Three – Data Protection and Information Security Questions for Suppliers of IT Solutions \* N/A**

**Section Four – Data Protection and Information Security Questions for Services utilising IT Solutions to capture data**

In addition to the core data protection and information security questions in step two, the table below sets out the additional requirements when dealing with contracts or services that utilise an IT solution (i.e. Customer Relationship Management CRM or appointment scheduler system) to capture personal data in the provision of such contracts or services.

|  |  |  |  |
| --- | --- | --- | --- |
| **4.** | **Expected Control – Data Retention and Disposal** | **Fully Compliant** | **Comments** **To be completed for all ‘No’ responses, including when the control is deemed to be not applicable, in accordance with ‘2. Instructions’ above.** |
| 4.1 | Do you have a contract in place with the supplier of the IT solution to use the software as part of the Council’s contract?  | Yes [ ]  | No [ ]  |  |
| 4.2 | Does the IT solution have a configurable password policy, which allows you to:• Configure a password history; • Configure a maximum password age; • Configure a minimum password age; • Configure a minimum password length (minimum of 12 characters);• Configure a account lockout threshold of invalid logon attempts• Configure password complexity requirements of at least four of the following elements:• Numeric – (0-9)• Uppercase – (A-Z)• Lowercase – (a-z)• Special Characters (?,!, @, #, %, etc…)• Spaces | Yes [ ]  | No [ ]  |  |
| 4.3 | Do you use multi-factor (2FA/MFA) authentication to access the system in the event that you hold special categories of data i.e. health records, safeguarding? | Yes [ ]  | No [ ]  |  |
| 4.4 | Do you have user guides and documentation to support the use of the IT solution? | Yes [ ]  | No [ ]  |  |
| 4.5 | Does the IT solution allow different user permissions to be assigned based on their role i.e. read only, amend or full administration? | Yes [ ]  | No [ ]  |  |
| 4.6 | Does the IT solution have an extractable audit trail which records the activity of users and system administrators including:-* Date and time of transaction;
* User ID and name of the individual undertaking the transaction;
* Details of the data before and after the transaction;
* Details of user ‘logins’, ‘logouts’ and failed user connections; and

Details of the user’s device IP address making the connection. | Yes [ ]  | No [ ]  |  |
| 4.7 | Is the IT solution subject to a periodic independent penetration test (i.e. annually) to highlight potential security issues? | Yes [ ]  | No [ ]  |  |
| 4.8 | Does the IT Solution have a login banner that provides a warning to potential intruders that certain types of activity is illegal and advises authorized users of their obligations relating to acceptable use of the system? | Yes [ ]  | No [ ]  |  |
| 4.9 | Is the location holding the IT solution and its data certified to the information security standard ISO27001:2013 or equivalent?  | Yes [ ]  | No [ ]  |  |
| 4.10 | Does the IT solution and its data which is provided as a cloud service, comply with the UK Government’s Cloud Security Principles, including compliance with ISO/IEC 27017 Security controls for Cloud Services? | Yes [ ]  | No [ ]  |  |
| 4.11 | Are procedures in place to enable the recovery of the IT solution and its data in the event of interruption to normal operational service?  | Yes [ ]  | No [ ]  |  |