

**Appendix B Information Security Requirements**

**Ref CCS030**

**Provision of Educational Psychology Assessments**

**Applicants Name:**

Contents

[1. Background 3](#_Toc122423505)

[2. Instructions 3](#_Toc122423506)

[3. Checks and Standards 5](#_Toc122423507)

# 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.

Individuals, organisations and the voluntary sector are integral in assisting the Council to deliver a variety of essential services across Derbyshire. To provide a number of these services, the Council is required to provide access to personal data in respect of the individuals to whom services will be provided. As a responsible organisation, the Council is required by law, to take reasonable steps to ensure that personal data covered by the DPA is protected against unauthorised access or loss. With this in mind, the Council has produced a checklist of the basic data protection and information security standards that are required where the storing, handling, processing and/ or retention of personal data are incidental to the service being provided.

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.

# Instructions

Tenderers are required to select the relevant response box (**Yes** or **No**) for each control in the table in Section 3; 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, or 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 assessment.

Responses to each control will be evaluated in accordance with the scoring criteria in the table below.

|  |  |
| --- | --- |
| **Result** | **Assessment Criteria**  |
| **Pass**  | The information /evidence has been assessed and judged to be acceptable. |
| **Fail** | Question not answered, or a no answer has been indicated ; and/orThe response does not meet the full criteria and there is limited information provided or an answer that largely fails to address the question or that is flawed in aspects; and/orThere are significant gaps and no evidence that services provided will be in line with expectations and the standards required.  |

# Checks and Standards (Pass/Fail)

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** |  **Paper Records and Confidentiality** | **In Place?** | **Comments**If you say no, please provide a comment to let us know why and when you think you will be able to achieve this. |
| **With reference to the Council’s confidential and/or personal data, please confirm you will:** |
| 1.1 | Safely lock away any paper records at the end of each working day. | Yes [ ]  | No [ ]  |       |
| 1.2 | Provide keys only to people who need them for this service. | Yes [ ]  | No [ ]  |       |
| 1.3 | Shred confidential and/or personal data when it’s no longer required. | Yes [ ]  | No [ ]  |       |
| 1.4 | Ensure that printers you use are only accessible to people involved in delivering this service.  | Yes [ ]  | No [ ]  |       |
| 1.5 | Ensure that all documents are retrieved and not left on communal or public printers, faxes and photocopiers. | Yes [ ]  | No [ ]  |       |
| 1.6 | Ensure the security of documents at all times and that they are not left unattended or able to be viewed by others when travelling. | Yes [ ]  | No [ ]  |       |
| **2.** | **Electronic Records and Confidentiality** | **In Place?**  | **Comments**If you say no, please provide a comment to let us know why and when you think you will be able to achieve this. |
| **With reference to the Council’s confidential and/or personal data, please confirm you will:** |
| 2.1 | Ensure that data is protected when sent electronically by the use of encryption and that documents and attachments including spreadsheets, letters and schedules are protected by the use of a minimum of 12-character passwords.  | Yes [ ]  | No [ ]  |       |
| 2.2 | Only send by fax where no other options are available. | Yes [ ]  | No [ ]  |       |
| 2.3 | Ensure that personal and/or confidential data is not sent via SMS, text or instant messaging services.  | Yes [ ]  | No [ ]  |       |
| 2.4 | Notify the Council immediately if data is lost, stolen, compromised, or accidentally given to someone who should not have it. | Yes [ ]  | No [ ]  |       |
| **3.** | **IT equipment and Confidentiality** | **In Place?**  | **Comments**If you say no, please provide a comment to let us know why and when you think you will be able to achieve this. |
| **With reference to the Council’s confidential and/or personal data, please confirm you will:** |
| 3.1 | Lock away laptops, USB devices, iPads etc., at the end of each working day.  | Yes [ ]  | No [ ]  |       |
| 3.2 | Install anti-virus software on IT equipment and ensure automatic updates is activated.  | Yes [ ]  | No [ ]  |       |
| 3.3 | Update software used on laptops, PCs, and mobile devices regularly by ensuring ‘automatic updates’ is enabled. | Yes [ ]  | No [ ]  |       |
| 3.4 | Secure mobile devices including phones and iPads with a ‘PIN’ or biometric identification. | Yes [ ]  | No [ ]  |       |
| 3.5 | Where possible, ensure devices such as PCs, laptops etc., are encrypted. | Yes [ ]  | No [ ]  |       |
| 3.6 | Dispose of old laptops, USB devices, iPads, smartphones etc., securely to ensure that the data on the hard drives is destroyed and cannot be recovered.  | Yes [ ]  | No [ ]  |       |
| 3.7 | Take all reasonable steps to ensure that the information is not accidentally or intentionally disclosed. | Yes [ ]  | No [ ]  |       |
| 3.8 | Ensure that personal and/or confidential data is not saved or stored on personal devices that do not belong to the organisation. | Yes [ ]  | No [ ]  |       |
| **4.** | **Staff** | **In Place?**  | **Comments**If you say no, please provide a comment to let us know why and when you think you will be able to achieve this. |
| **With reference to the Council’s confidential and/or personal data, please confirm you will:** |
| 4.1 | Ensure awareness and compliance with the data protection responsibilities of the service. | Yes [ ]  | No [ ]  |       |
| 4.2 | Provide anyone involved in delivering the service with an induction that includes information security and data protection awareness and guidance.  | Yes [ ]  | No [ ]  |       |
| 4.3 | Provide anyone involved in delivering the service with an annual update and awareness of the organisation’s data protection and information security procedures.  | Yes [ ]  | No [ ]  |       |
| **5.** | **Business Continuity** | **In Place?**  | **Comments**If you say no, please provide a comment to let us know why and when you think you will be able to achieve this. |
| **With reference to the Council’s confidential and/or personal data, please confirm you will:** |
| 5.1 | In the event of any disruption to the service, ensure you can access details of any key activities and contacts relating to planned sessions, which you could use to provide any updates. | Yes [ ]  | No [ ]  |       |