Information Security Document

Supplier Information Security Policy

Version 8.0

Version	Date	Detail	Author
1.0		Completed for distribution	Jo White
1.1	24/08/2015	Legal comments	Simon Hobbs
1.2	24/08/2015	Commissioning comments	Ruth Wildgoose
2.0	03/09/2015	Agreed by Information Governance Group	Jo White
3.0	11/07/2016	Reviewed by Information Governance Group.	Jo White
4.0	06/11/2017	Reviewed by Information Governance Group. IS contact for small businesses added.	Jo White
5.0	04/12/2017	Reviewed by Information Governance Group. GDPR and PIAs added.	Jo White
6.0	07/01/2019	Reviewed by Information Governance Group. Page 16, new 5.5 and 5.10 added.	Jo White
7.0	11/08/2020	Revised wording added under Purpose regarding GDPR, amendment regarding the Council's Financial Regulations, changes to Appendix A and B. Appendix C added.	Information Security Team, Audit Services & Procurement.
8.0	02/11/2021	Reviewed by Information Governance Group. Amendments in line with feedback from suppliers.	Information Security Team, Audit Services & Procurement.

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.15	Supplier Relationships
A.18	Compliance

1. Introduction

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. To enable this, it is essential that information is secured in accordance with professional best practice including statutory, regulatory and contractual requirements that maintain the confidentiality, integrity and availability of all information assets.

The Council is certified to the Information Security Management standard ISO27001:2013 and has an established Information Security Management System (ISMS) in accordance with the requirements of ISO27001 and ISO27002 code of practice for information security controls. The ISMS provides an important framework to assist the Council in meeting its data protection obligations under the General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA).

2. Purpose

The purpose of this policy, is to put procedures in place to ensure that contracts and dealings between the Council and third party suppliers have acceptable levels of data protection and information security in place to protect both personal and business confidential data. The GDPR places statutory obligations on data controllers and processors who are involved in the processing of personal data.

The GDPR draws a distinction between a 'Controller' and a 'Processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The GDPR defines these terms:

- '**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- '**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- Where two or more controllers jointly determine the purposes and means of processing, they shall be '**Joint Controllers'**.

As a data controller, the Council is responsible for complying with the GDPR and must be able to demonstrate compliance with the data protection principles. This will include taking appropriate technical and organisational

measures to ensure personal data processing is carried out in accordance with current data protection legislation.

In the majority of instances, the relationships between the Council and its third party suppliers are ultimately governed by a contract or information sharing agreement, which is entered into between the Council and the third party supplier.

3. Scope

The scope of this policy applies to contracts, service arrangements, grant awards and partnership agreements that involve IT solutions or the provision of services which require access to, or the processing of, personal and/or business confidential data for the delivery and/or support of Council services and business functions. The term '**processing of personal data'**, within this policy refers to either:-

a) the storing, handling, processing or retention of data including personal data related to the Council's information e.g. employee, elected member and client records. Examples include, but not limited to, the procurement of major IT solutions for Payroll, Care Records, Educational Monitoring etc., or

b) the storing, handling, processing or retention of data - including personal data related to/associated with the services commissioned by the Council. Examples of which include Public Health contracts.

4. Policy Statement

The Council has robust and well-established procurement processes which are designed to ensure solutions and services procured are cost effective, maintain the confidentiality, integrity and availability of information and are fit for purpose. It is therefore important that throughout the procurement and subsequent contractual period, the Council and its providers are clear on the Council's expectations in terms of data protection, information security and supplier responsibilities.

5. Third Parties – Data Protection and Information Security Obligations

The security of information is fundamental to the Council's compliance with current data protection legislation and a key focus in its ISO27001:2013 risk assessment, procurement and management strategy.

The Council uses a risk based and proportionate approach to how information assets should be protected. Having procurement processes which align with identified information asset risks helps to ensure that services and IT solutions are procured, which are able to provide the level and quality of information security required by the Council and are compliant with current data protection legislation. To assess the level of risk, all projects which involve the collection,

processing or storage of personal data are required to be supported by the completion of a Data Protection Impact Assessment (DPIA). DPIAs must be created for all new projects or significant revisions of existing projects. Where appropriate, the Council will identify the need for a DPIA at an early stage and build this into project management or other business processes. The client department (Commissioner) will be responsible for the creation and as living documents, the ongoing review and monitoring of the DPIA. The completed document should be presented to the Information Governance Group (IGG) for review and monitoring purposes. Additional guidance can be found in the Council's DPIA Procedures.

Two procurement approaches have been developed for use in the procurement of contracts, services and awarding of grants/ partnership agreements, which include personal and business confidential data. The use of these approaches is driven by the nature of the service and the sensitivity, volume and risk associated with the information held.

a) <u>Major IT solutions and contracts that involve the processing and / or retention of high volume of personal data</u>.

Where 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".

The table below provides guidance on the Council's classification methodology. This also defines the information security and data protection requirements that potential suppliers will be asked to meet as part of the procurement process. The individual information security and data protection requirements are detailed in ***Appendix A***.

Type of Personal Data Restricted Data	Type of Personal Data Controlled Data	Type of Personal Data Public Data
The solution or service involves the storage or processing of special categories of personal data. • racial or ethnic origin, • political opinions, • religious or philosophical beliefs, or • trade union membership, and • the processing of genetic data, biometric data for the purpose of uniquely	The solution or service involves the storage or processing of information relating to an identified or identifiable natural person ('data subject').	The solution or service has very limited personal data or does not involve the storage or processing of any personal data.

Type of Personal Data Restricted Data	Type of Personal Data Controlled Data	Type of Personal Data Public Data
identifying a natural person, • data concerning health or • data concerning a natural person's sex life or sexual orientation.		

N.B. Unless otherwise determined, all new IT solutions, inventory applications and services (or significant enhancements) which capture, process or hold financial, or business confidential information will be classified as **Controlled Data**.

5.1 Cyber Security

Unless able to apply an exemption, Council contracts for major IT solutions and contracts that involve the processing and/ or retention of high volume of personal data, will include a requirement for the supplier to be certified under the government-backed Cyber Essentials scheme as a minimum. The rationale for the Council's approach to Cyber Essentials is based on:

- The Government's Procurement Policy Note 09/14 – Cyber Essentials Scheme, mandated Cyber Essentials for contracts advertised after 1 October 2014;
- The Information Commissioner's Office refers to the Cyber Essentials Scheme as a method by which an organisation can assess their systems and implement specific technical controls in line with GDPR;
- The National Cyber Security Centre guidance on supply chain security, refers to building *'assurance measures into your minimum security requirements (such as Cyber Essentials Plus, audits and penetration tests). These provide an independent view of the effectiveness of your suppliers security'*;
- The Local Government Association includes guidance on the Cyber Essentials scheme as one of three ways to specify evidence for safe and secure handling of information in contracts.

Where the contract requires the processing of high risk or large volumes of special categories of personal data (as defined within the DPA) consideration should be given to the supplier being accredited against the Cyber Essentials 'Plus' certification. The exemptions applied by the Council are detailed below:-

- G-Cloud: Cloud services procured through G-Cloud are assessed against Government's Cloud Service Security Principles.
- Digital Services Framework (DSF): DSF suppliers have been technically and commercially evaluated to provide a comprehensive choice for agile projects.

- Public Sector Network (PSN): PSN services are currently accredited against the network's security standards. In the future, PSN services will be assessed against Government's Network Security Principles.
- ID Assurance Framework: Being able to provide your identity online easily, quickly and safely is recognised as a key enabler of internet use by the Government and its users. Providers of public services such as national and local governments, major internet companies, online retailers, banks and others have to address business and security issues around identity proofing and username/password fallibility to mitigate the financial and administrative implications of identity fraud and compromise of personal data.
- Assisted Digital: Assisted Digital is support for people who can't use online services independently.
- Suppliers conforming to the ISO27001 standard where the Cyber Essentials requirements, at either basic or Plus levels as appropriate, (see paragraph 1 above) have been included in the scope, and verified as such, would be regarded as holding an equivalent standard to Cyber Essentials and Cyber Essentials Plus.
- Organisations that have been certified against the NHS Data Security and Protection Toolkit 2020-21 (DSPT).

As the Cyber Essentials Scheme covers the principles of computer and internet connectivity, a number of very small organisations which have limited IT support or may use paper based processes, will not fall under these requirements.

b) <u>Contract, grant awards and partnership agreements where the use, processing and retention of data is incidental to the service being provided.</u>

Where the storing, handling, processing and/ or retention of personal or business confidential data is incidental to the service being provided**,** suppliers will be asked to meet the requirements listed at ***Appendix B***. This may include the issue of grant monies and commissioning of services whose primary focus is to support small groups of individuals in the community and promote local well-being projects.

5.2 Approval from the Director of Finance & ICT

The Council's Financial Regulations (2019) require that *"The Chief Financial Officer is responsible for the operation of the Council's accounting systems, the form of accounts and the supporting financial records. Any proposed changes by Strategic Directors to existing financial and/or control systems or the establishment of new systems must be reported to and considered by the Assistant Director of Finance (Audit) who will consider the potential impact on the Internal Control framework and report to the Chief Financial Officer, raising any concerns as appropriate. The Chief Financial Officer will then formally consider the proposed changes. No changes may be actioned without the formal approval of the Chief Financial Officer."*

5.3 Information Security Due Diligence

As far as possible, due diligence checks proportionate to the risk of the processing, are undertaken before a contract is agreed with a processor or third party supplier. The due diligence process includes data security checks, external data centre/ office site visits, system testing and audit requests. This process supports the Council to demonstrate appropriate technical and organisational measures are in place in line with current data protection requirements.

To enable this, new IT system projects, significant changes to existing systems or services categorised as 'Restricted' or 'Controlled' above, should be notified to Audit Services to determine the level of assessment required.

The objective of the site visit(s) will be to assess the adequacy of the physical, logical and operational controls in place and assess whether the supplier's approved IT security and data protection procedures are embedded within day to day operations. Where applicable, a review of the IT system's control framework may also be undertaken, prior to being installed by the Council.

At the conclusion of the Audit due diligence the data protection and information security issues will be communicated to the third party supplier for comment. At this point the supplier has the opportunity to provide a response on the issues that have been identified and include an appropriate actions regarding how the control/ weakness will be addressed (including a timeframe for correction). In the event that the supplier's response is satisfactory, with an appropriate timeframe for the correction of the identified issues, the Director of Finance & ICT will be provided with an Audit report detailing the associated findings for consideration. Details of the information security issues and supplier's response will be included within the Council's contract to enable the implementation of agreed information security controls to be monitored. A flowchart outlining the key steps is included at **Appendix C**.

5.3 Contracts

All Council contracts shall clearly define each party's data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the classification of the data, various additional information security controls may be incorporated within the contract in addition to those set out either in **Appendix A** or **B** dependent upon the nature of the service provision. The DPA includes details on the Council's obligations in terms of contractual requirements with data processors:

The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following:-

(a) the subject-matter and duration of the processing;
(b) the nature and purpose of the processing;
(c) the type of personal data and categories of data subjects involved;
(d) the obligations and rights of the controller and processor.

6. Management of Supplier Relationships

During the period of the contract or relationship term, the Council will manage the arrangement with its third party suppliers to ensure data protection and Information Security standards are maintained. Where Audit Services have undertaken an information security review, which resulted in recommendations being made to the supplier, the implementation of these, should be monitored during contract review meetings.

6.1 Sub-Contracting

The Council will include appropriate contractual obligations to ensure that any sub-contractor engaged by a third party supplier is required to operate to the same data protection and Information Security standards as the primary contractor. Where there is a change in the delivery of a contract with the main contractor seeking to sub-contract all or part of the Council's contract this must be formally approved by the Council prior to any changes.

6.2 Supplier Access to Council Information

The Council will allow third party suppliers to access its information and data, where formal contracts and data sharing agreements exist in accordance with current data protection legislation, the Council's ISMS and where:

- Accessing the information is an agreed part of the solution/service provided.
- The processing and viewing of information is necessary for maintenance and trouble-shooting of the solution being provided.
- Information may need to be reconstructed, repaired or restructured.
- Information has been provided for inclusion in the solution/service by the Council.
- Information may need to be transferred to other systems or during IT solution upgrades.
- Information may need to be collected with agreement from, and on behalf of, the Council.

Viewing (i.e. access not agreed by the Council) of Council information is not permitted at any time by third party suppliers. Council information must not be accessed under any circumstances unless formal information sharing agreements or written contractual permissions have been established between the parties which permit this to happen.

The extent of third party supplier requirements to access Council information will need to be identified prior to any contractual obligations being established and entered into. The level and type of access to Council information by third party suppliers must also be formally agreed by the parties. The security requirements for each type of information will be defined within all tender and contract documentation and the security of the information must be handled in accordance with the Council's Information Classification and Handling Policy.

The Council is very clear that where there is a requirement for the processing of personal data of employees or service users by third parties, information must be treated in accordance with the Council's data protection obligations and requirements to ensure the confidentiality, integrity and availability of all information.

6.3 Monitoring Supplier Access to the Council's Network

IT solutions which are hosted on the Council's network will be subject to periodic checks to ensure that any external access by third party suppliers for support and maintenance is monitored. Once the required work has been undertaken by the third party, access to the account will be disabled and the password changed. Each instance of support and maintenance connections required by the third party supplier will need to be formally approved by the Council before being provided.

7. Security Incident Management

Third party suppliers will be expected to have appropriate security incident management procedures in place, which correspond to the level of service being provided, sensitivity of the data and GDPR requirements. The extent of these responsibilities will be specified in the contract or data sharing agreement. Third party suppliers will be required to notify the Council of any significant security incidents as soon as practical.

8. Notification of a personal data breach to the Commissioner

Under the DPA, the Council and its third party suppliers have a duty, to report certain types of data breach to the Information Commissioner's Office. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

As a notifiable breach is required to be reported within 72 hours of an organisation becoming aware of it, any such instances must be reported

through the Council's Incident Reporting procedure immediately. Failure to do so could result in significant monetary fines being levied on the Council.

9. Suspension of the Supplier Information Security Policy

As part of the Council's ISO27001:2013 framework the Policy is subject to annual review and update. However, it is important that the Council has a mechanism in place to enable elements of the Policy's requirements to be suspended within this period, should there be a significant or adverse impact on the Council's services/ procurements.

In such instances and following consideration of the available facts, the Director of Finance & ICT will make a decision regarding whether the requirements of the Policy are suspended until the Information Governance Group have the opportunity to review its impact.

10. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council information assets, or an event which is in breach of the Council's security procedures and policies. All third party suppliers contracted to provide, support or access solutions, which enable the Council to carry out its business functions and deliver its services, have a responsibility to adhere to this policy and all supporting requirements as described and referenced within formal documentation and agreed contractual agreements.

All employees, elected members and volunteers have a responsibility to report security incidents and breaches of this policy within 24 hours of becoming aware of the incident through the Council's Incident Reporting Procedure

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to IT solutions or suspension/ termination of contractual arrangements. If damage or compromise of the Council's IT solutions or loss of information results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of this policy and its associated procedures and guidelines through the relevant contractual arrangements in place or otherwise via statutory processes. In the case of an employee, infringements will be investigated under the Council's disciplinary procedure and progressed as appropriate.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.

The Council's information security and data protection requirements for potential third parties and suppliers are split over four distinct areas:

- Part One - To be completed by all third parties and suppliers
- Part Two – To be completed by all third parties and suppliers
- Part Three – To be completed by third parties and suppliers who will be providing, or utilising IT systems or solutions installed on the Council's internal network or hosted remotely by the supplier (. e.g procurement of a Payroll system for use by the Council)
- Part Four **–** To be completed by third parties and suppliers who will be utilising third party/cloud based IT systems or solutions in the delivery of the contract (e.g external supplier utilising an in-house Customer Relationship Management (CRM) system to deliver services on behalf of the Council)

Note:
When completing Parts Three and/or Four, it is essential that third parties and suppliers consider the storage of all data associated with the delivery of the contract and where this may be located. This may include, word documents, spreadsheets, emails, photos or other online records that may be stored outside of the core IT system.

Part One – Independent Information Security Certification (To be completed by all Suppliers)

Unless able to apply an exemption, Council contracts for major IT solutions and/or contracts that involve the processing and/or retention of high volume of personal data, will include a requirement for the supplier to be certified under the government-backed Cyber Essentials scheme. Where the contract requires the processing of special categories of personal data, as defined within the DPA, consideration should be given to the supplier being accredited to the Cyber Essentials Plus certification. 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.

Ref.	Expected Control – Cyber Essentials	Restricted Data	Controlled Data	Public Data
1.1	Where deemed necessary, the supplier holds a current 'Cyber Essentials Plus' certification (or equivalent)	✓	X	X
1.2	The supplier holds a current 'Cyber Essentials' certification (or equivalent)	X	✓	X

	Support and Guidance provided by Audit Services		Support and Guidance provided by the Information Security/Governance Team

Part Two – Core Data Protection and Information Security Questions (To be completed by 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 and/or business confidential data by third parties (including suppliers, contractors, sub-contractors and employees). The expected controls aim to protect the Council's interests by providing a flexible approach to managing data protection and information security risks during contractual arrangements. Where there is a requirement to remove an expected control from an individual procurement this must be documented as part of the procurement planning and management process.

Ref.	Expected Control – Staff Related	Restricted Data	Controlled Data	Public Data
2.1	Do you have written contracts of employment for your staff, which include reference to your information security policies and procedures?	✓	✓	X
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?	✓	✓	X
2.3	Are your staff, volunteers and agency workers provided with annual training/ updates on information security and data protection?	✓	✓	X

Ref.	Expected Control – Policies	Restricted Data	Controlled Data	Public Data
2.4	Do you have information security policies in place which your staff, volunteers and agency workers are required to comply with?	✓	✓	✓
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?	✓	✓	✓
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?	✓	✓	✓
2.7	Are staff, volunteers and agency workers trained not to disclose their password to anyone?	✓	✓	✓
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?	✓	✓	✓
2.9	Are staff, volunteers and agency workers restricted from using personal equipment (i.e. laptops, phones, USB devices) for business activities?	✓	✓	✓
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?	✓	✓	X
2.11	Do you have a Homeworking Policy for all staff, volunteers and agency workers?	✓	✓	✓
2.12	Have you undertaken a risk assessment in terms of information security and Homeworking arrangements?	✓	✓	✓
Ref.	**Expected Control – User Permissions**	**Restricted Data**	**Controlled Data**	**Public Data**
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?	✓	✓	✓
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?	✓	✓	✓
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?	✓	✓	X
Ref.	**Expected Control – Network**	**Restricted Data**	**Controlled Data**	**Public Data**
2.16	Do you have a firewall (or similar network device) installed on the boundary of your internal network?	✓	✓	✓
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?	✓	✓	✓
2.18	Is anti-virus and malware software installed and regularly updated on all of your IT equipment (i.e. servers, computers and laptops)?	✓	✓	✓
2.19	Are all your computers and devices hard drives protected by encryption (e.g. Windows Bitlocker)?	✓	✓	✓
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)	✓	✓	✓
2.21	Do you have the ability to send and receive secure, encrypted emails when communicating/exchanging restricted or confidential data with the Council?	✓	✓	X
2.22	Do you undertake an annual vulnerability scan of your internal network to highlight potential security issues?	✓	X	X
2.23	Do you undertake an annual vulnerability scan of your external network to highlight potential security issues?	✓	✓	✓
2.24	Do you retain audit logs from your Internet, server and IT network usage for at least 30 days?	✓	✓	✓
2.25	Do you restrict staff from sending confidential or personal data via SMS, text or instant messaging services?	✓	✓	X
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’	✓	✓	X
Ref.	**Expected Control – Patch Management**	**Restricted Data**	**Controlled Data**	**Public Data**

2.27	Do you apply security patches (e.g Microsoft Windows updates) to all software running on your computers and network devices?	✓	✓	✓
2.28	Has out of date software been removed from your computers and network devices (e.g Windows XP or Windows 7)?	✓	✓	✓
2.29	Do you apply vendor updates and application updates to your smart phones?	✓	✓	X
Ref.	**Expected Control – Business Continuity**	**Restricted Data**	**Controlled Data**	**Public Data**
2.30	Do you have a Disaster Recovery and Business Continuity Plan in place for your organisation?	✓	✓	✓
2.31	Do you periodically test (at least annually) your Disaster Recovery and Business Continuity Plan?	✓	✓	✓
2.32	Do you regularly take backups of your IT systems and its data?	✓	✓	✓
2.33	Are your backups protected by encryption and held in a separate location to the main data?	✓	✓	✓
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)?	✓	✓	X
Ref.	**Expected Control – Data Retention and Disposal**	**Restricted Data**	**Controlled Data**	**Public Data**
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?	✓	✓	X
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?	✓	✓	✓
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?	✓	✓	X
Ref.	**Expected Control – Manual Records**	**Restricted Data**	**Controlled Data**	**Public Data**
2.38	Are all paper records containing the confidential or personal data held securely on-site or as part of off-site storage facilities?	✓	✓	X
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?	✓	✓	X
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?	✓	✓	✓
Ref.	**Expected Control – Legal Compliance**	**Restricted Data**	**Controlled Data**	**Public Data**
2.41	Do you have procedures in place to monitor compliance with the Data Protection Act 2018 and General Data Protection Regulation?	✓	✓	✓
2.42	Do you have procedures in place to monitor compliance with the Computer Misuse Act (1990)?	✓	✓	✓
2.43	Do you have procedures in place to monitor compliance with the Privacy and Electronic Communications Regulations (2019)?	✓	✓	✓
Ref.	**Expected Control – Third Parties**	**Restricted Data**	**Controlled Data**	**Public Data**
2.44	Do you have contracts in place with all of your third party suppliers i.e. IT support or data hosting company?	✓	✓	✓
2.45	Have you undertaken appropriate due diligence checks (including the review of information security accreditations where appropriate i.e.– Cyber Essentials) on third party suppliers that have access to personal data i.e. IT support and CRM system providers?	✓	✓	X

	Support and Guidance provided by Audit Services		Support and Guidance provided by the Information Security/Governance Team

Part Three – Data Protection and Information Security Questions for Suppliers of IT Solutions or Services either Hosted on the Council's Network or Externally by the Supplier

In addition to the core data protection and information security questions in parts one and two, the table below sets out the additional requirements when dealing with contracts or services that relate to the provision or use of IT systems or solutions:

- installed on the Council's internal network; or
- hosted remotely by the supplier.

- Where there is a requirement to remove an expected control from an individual procurement this must be documented as part of the procurement planning and management process

Ref.	Expected Control – Access	Restricted Data	Controlled Data	Public Data

3.1	Does the IT solution have a configurable password policy, which would allow the Council 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
		✓	✓	✓

3.2	Can the IT solution's administrative accounts (i.e. change of the system administrator's password) be undertaken without updates to the software?	✓	✓	✓
3.3	Does the IT solution have the ability to enable multi-factor (2FA/MFA) authentication that can be configurable to apply to each login instance if required, and include support for other methods of User authentication for example, Active Directory, Single Sign-on use of an existing Federation Service etc.?	✓	✓	X
3.4	Do you have user guides and documentation to support the installation and use of the IT solution?	✓	✓	✓
3.5	When installing new IT systems do you ensure 'Live' data is not be used in any test systems?	✓	✓	X
3.6	Does the IT solution allow different user permissions to be assigned based on their role i.e. read only, amend or full administration?	✓	✓	✓
3.7	Do you have procedures to ensure that data transferred from the Council's existing IT systems are undertaken securely (i.e. use of encryption)	✓	✓	X
3.8	Does the IT solution have an extractable audit trail which records the activity of users and system administrators including:-	✓	✓	✓

Ref.	Expected Control – Access	Restricted Data	Controlled Data	Public Data
	• 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			
3.9	Is the IT solution subject to a periodic independent penetration test (i.e. annually) to highlight potential security issues?	✓	✓	✓
3.10	Does the IT Solution have a login banner that provides a warning to potential intruders that certain types of activity is illegal and advises authorised users of their obligations relating to acceptable use of the system?	✓	✓	✓
3.11	Are procedures in place to record access to the IT Solution for system maintenance and/or system administration support, which include details of the activity undertaken?	✓	✓	✓
3.12	Does the IT Solution include the provision of a Mobile App which has been developed to ensure personal and/or business confidential data is protected using secure access/communication technologies and regularly updated with security updates/patches? ***(Question to be used if the provision of a mobile app forms part of the specification)***	✓	✓	X
3.13	Is the location holding the IT solution and its data certified to the information security standard ISO27001:2013 or equivalent? ***(Externally Hosted IT Solutions only)***	✓	✓	X
3.14	Does the IT solution and its data which is provided as a cloud service, comply with the UK Government's Cloud Security Principles and/or compliance with ISO/IEC 27017 Security controls for Cloud Services?	✓	✓	X
3.15	Are procedures in place to enable the recovery of the IT solution and its data in the event of interruption to normal operational service? ***(Externally Hosted IT Solutions only)***	✓	✓	✓

	Support and Guidance provided by Audit Services		Support and Guidance provided by the Information Security/Governance Team

Part Four – Data Protection and Information Security Questions for Suppliers utilising a Third Party and/or Cloud based IT System or Solution in the Delivery of the Contract

In addition to the core data protection and information security questions in parts one and two, the table below sets out the additional requirements when dealing with contracts or services where the supplier will be utilising a third party/cloud based IT systems or solutions in the delivery of the service/contract:

- that are cloud based or
- hosted by a third party

Where there is a requirement to remove an expected control from an individual procurement this must be documented as part of the procurement planning and management process.

Ref.	Expected Control – Access	Restricted Data	Controlled Data	Public Data
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?	✓	✓	✓

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
		✓	✓	✓

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?	✓	✓	X
4.4	Do you have user guides and documentation to support the use of the IT solution?	✓	✓	✓
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?	✓	✓	✓
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.	✓	✓	✓
4.7	Is the IT solution subject to a periodic independent penetration test (i.e. annually) to highlight potential security issues?	✓	✓	X
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?	✓	✓	✓
4.9	Is the location holding the IT solution and its data certified to the information security standard ISO27001:2013 or equivalent?	✓	✓	X
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?	✓	✓	X
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?	✓	✓	✓

	Support and Guidance provided by Audit Services		Support and Guidance provided by the Information Security/Governance Team

Additional guidance or clarification on the requirements within **Appendix A** can be obtained from the Council’s Information Security/Governance Team using the following contact details:
Telephone: (01629) 538984 **Email:** security.team@derbyshire.gov.uk

Appendix B
Data Protection and Information Security Guidance

PUBLIC

BACKGROUND

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 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.

1.	**Paper Records and Confidentiality**	**In Place**
1.1	Paper records containing the Council's confidential or personal data must be locked away at the end of each working day.	Yes/ No
1.2	Keys used to keep the Council's information secure should only be provided to individuals who need them for their job.	Yes/ No
1.3	The Council's confidential or personal data must be shredded when no longer required.	Yes/ No
1.4	Printers and faxes used for the Council's confidential or personal data should only be available to individuals who need access to undertake their role.	Yes/ No
1.5	The Council's confidential or personal data should not be left on printers, faxes, photocopiers.	Yes/ No
1.6	When transporting the Council's confidential or personal data by vehicle all records must be held securely when left unattended.	Yes/ No
2.	**Electronic Records and Confidentiality**	**In Place**
2.1	The Council's confidential or personal data sent electronically including spreadsheets, letters and schedules must be protected with a minimum of a 12 character password.	Yes/ No
2.2	The Council's confidential or personal data should only be sent by fax where no other options are available.	Yes/ No
2.3	The Council's confidential or personal data should not be sent via SMS, text or instant messaging services.	Yes/ No
2.4	In the event that the Council's confidential or personal data is lost, stolen or accidentally given to someone who should not have it, the Council must be notified as soon as possible.	Yes/ No
3.	**IT equipment and Confidentiality**	**In Place**

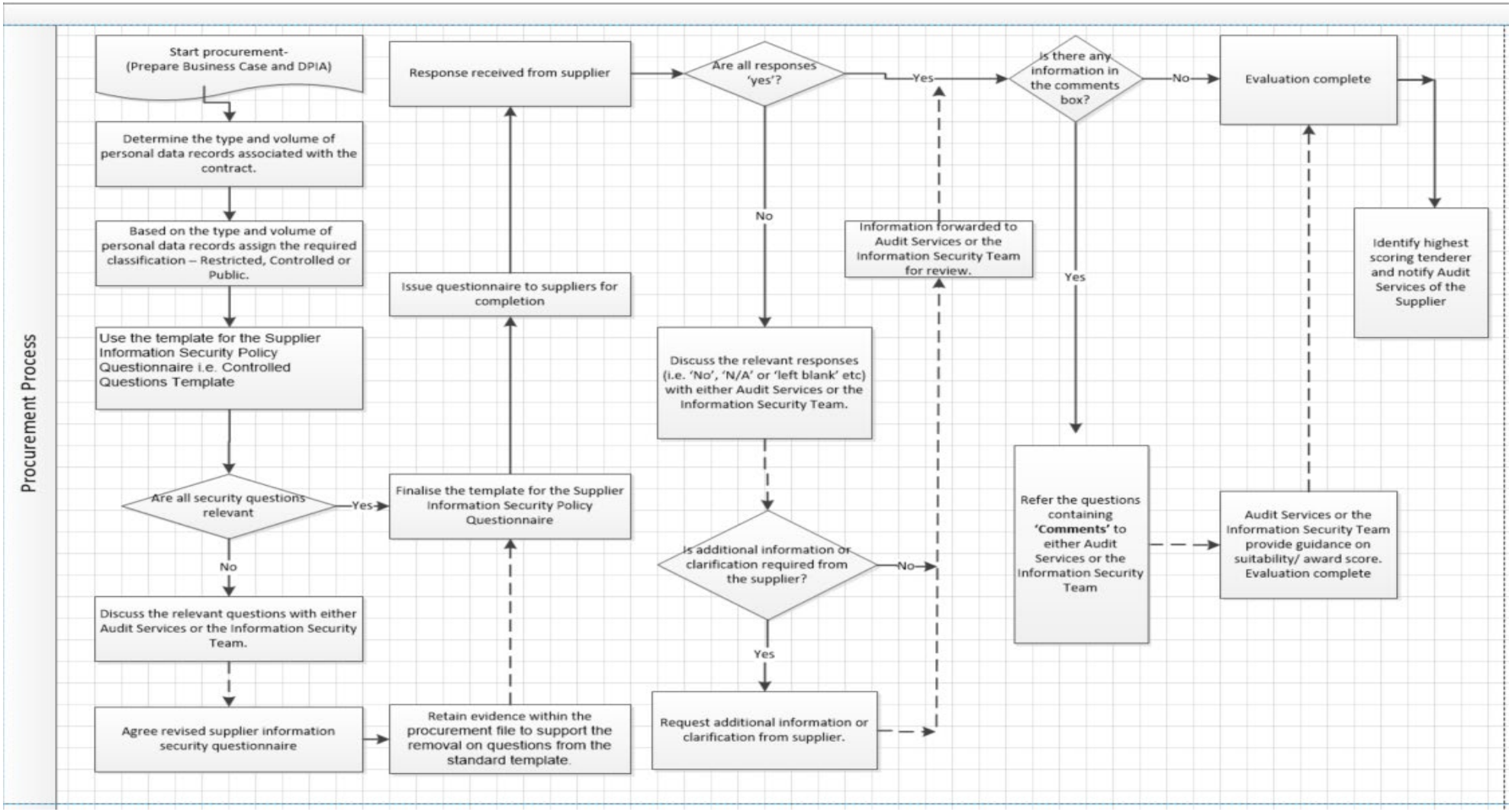
Appendix B
Data Protection and Information Security Guidance

3.1	Laptops, USB devices, iPads etc holding the Council's confidential or personal data must be locked away at the end of each working day.	Yes/ No
3.2	Anti-virus software must be installed on IT equipment holding the Council's confidential or personal data with the automatic update activated.	Yes/ No
3.3	Software used on laptops, PCs, and mobile devices should be updated regularly.	Yes/ No
3.4	Mobile devices including phones and iPads holding the Council's confidential or personal data must be secured by the use of a 'PIN'.	Yes/ No
3.5	Where possible, PCs and laptops holding the Council's confidential or personal data should be encrypted.	Yes/ No
3.6	Old laptops, USB devices, iPads, smartphones etc used to hold the Council's confidential or personal data must be disposed of securely to ensure that the data on the hard drives is destroyed.	Yes/ No
3.7	Individuals with access to the Council's confidential or personal data must take all reasonable steps to ensure that the information is not accidentally or intentionally disclosed.	Yes/ No
3.8	The Council's confidential or personal data should not be saved onto personal devices that do not belong to the organisation	Yes/ No
4.	**Staff**	
4.1	All staff, volunteers and agency workers should be aware of their data protection responsibilities when dealing with the Council's confidential or personal data?	Yes/ No
4.2	All staff, volunteers and agency workers should be provided with an induction that includes information security and data protection guidance.	Yes/ No
4.3	All staff, volunteers and agency workers should be provided with an annual update on the organisation's data protection and information security procedures.	Yes/ No
5.	**Business Continuity**	
5.1	A list of key tasks and contacts should be maintained in the event of a disruption to the operation of the organisation and its services.	Yes/ No

Additional guidance or clarification on the requirements within **Appendix B** can be obtained from the Council's Information Security/Governance Team using the following contact details:
Telephone: (01629) 538984 **Email:** security.team@derbyshire.gov.uk

Appendix C
Procurement Process

PUBLIC



Appendix C
Audit Due Diligence Process and Reporting

PUBLIC