Information Security Document

Supplier Information Security Policy

Important Note

This Policy has been produced based on current General Data Protection Regulations (GDPR) information and the Data Protection Bill (DPB). As further updates are released this Policy will be amended to reflect the changes.

Version History			
Version	**Date**	**Detail**	**Author**
1.0		Completed for distribution	
1.1		Legal comments	
1.2		Commissioning comments	
2.0		Agreed by Information Governance Group	
3.0		Reviewed by Information Governance Group.	
4.0		Reviewed by Information Governance Group. IS contact for small businesses added.	
5.0		Reviewed by Information Governance Group. GDPR and PIAs added.	

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 line with professional best practice as well as statutory, regulatory and contractual requirements that maintain the confidentiality, integrity and availability of all information assets.

The Council has 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. The ISMS will assist the Council to meet its data protection obligations under the General Data Protection Regulations (GDPR) and Data Protection Bill (DPB).

2. Purpose

The purpose of this policy is to put in place procedures so that contracts and dealings between the Council and third party suppliers have acceptable levels of data protection and information security in place to protect personal data. The new DPB places clear statutory obligations on data controllers and processors who are involved in the processing of personal data. The following are extracts from the DPB.

54. General obligations of the controller

(1) Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part.

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.
(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

(a) meet the requirements of this Part, and
(b) ensure the protection of the rights of the data subject

(3) The processor used by the controller may not engage another processor ("a sub-processor") without the prior written authorisation of the controller, which may be specific or general.

In the majority of instances, the relationships between the Council and its third party suppliers are ultimately governed by the 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 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 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, availability and integrity 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 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 solutions are procured, which are able to provide the level and quality of information security required by the Council and 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 privacy impact assessment (PIA). PIAs will be applied to new projects or revisions of existing projects. The Council will identify the need for a PIA at an early stage and build this into project management or other business processes. The client department (Commissioner) will be responsible for creating the PIA and submitting the completed document to the Information Governance Group (IGG) for monitoring purposes. Additional guidance can be found in the Council's PIA Procedures.

Two procurement approaches have, therefore, been developed for use in the procurement of contracts and the awarding of grants awards/ partnership agreements which include personal data. The use of these approaches is driven by the nature of the service, its integrity to the service that is required 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 GDPR 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 will also define 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	Type of Personal Data	Type of Personal 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	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 does not involve the storage or processing of any personal data.

Type of Personal Data	Type of Personal Data	Type of Personal Data
purpose of uniquely identifying a natural person, • data concerning health or • data concerning a natural person's sex life or sexual orientation		
Classification – **Restricted Data** (Appendix A)	Classification – **Controlled Data** (Appendix A)	Classification – **Public Data** (Appendix A)

Unless otherwise determined, all new IT solutions, inventory applications and services (or significant enhancements) which capture, process or hold financial or business 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 be certified under the government-backed Cyber Essentials scheme. Where the contract requires the processing of special categories of personal data, as defined within GDPR, the requirement will be for the supplier to have 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. Therefore suppliers in this situation are exempt, provided that the certification body (likely to be a consultancy) carrying out this verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies.

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

Where the storing, handling, processing and/ or retention of personal 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 wellbeing projects.

5.2 Approval from the Director of Finance & ICT

The Council's Financial Regulations 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."*

All 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 Audit assessment may necessitate a visit to the third party supplier's data centre and/or main office where access to, or processing of, personal data is being undertaken on behalf of the Council.

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 review the data protection and information security issues will be communicated to the supplier for comment. At this point the supplier has the opportunity to provide a response to Audit Services on the issues that have been identified and include an appropriate response on 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 provided 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.

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 DPB 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 the third party supplier to ensure data protection and Information Security standards are maintained.

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.

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

The DPB will introduce a duty on the Council and its third party suppliers, 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. 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 forms part of the Council's ISMS Policy and as such, must be fully complied with.

APPENDIX A

BACKGROUND

This document 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 personal 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.

1.	**Expected Control - Human Resource Security**	**Restricted Data**	**Controlled Data**	**Public Data**
1.1	Staff with access to the **Data** must have a written contract of employment under which they agree to adhere to information security policies, including a staff acceptable use policy.	✓	✓	X
1.2	Staff with access to the **Data** must receive an induction and have a continuous training programme that includes information security and data protection guidance throughout their employment.	✓	✓	X
1.3	Staff must not transfer the **Data** to personal email accounts or personal cloud based storage.	✓	✓	X
2.	**Expected Control - Physical and Environmental Security**	**Restricted Data**	**Controlled Data**	**Public Data**
2.1	The infrastructure hosting the **Data** must be classified as Tier 2 or above.	✓	X	X
2.2	The infrastructure hosting the **Data** must be certified to the information security standard ISO27001:2013 or equivalent.	✓	X	X
2.3	Physical access procedures must be in place to control access to sites hosting the **Data** to reduce the risk of unauthorised access, damage or theft and include:- • Visitor signing in procedures; • CCTV coverage of exit/entry points and data hosting environments; and • Alarm systems (including environment sensors) covering the hosting environment of the solution.	✓	✓	X

3.	Expected Control – Access Security	Restricted Data	Controlled Data	Public Data
3.1	IT solutions that record or process the **Data** must ensure that:- • Individual accounts are granted with minimum privileges to provide the service; • Default accounts are deleted or disabled; • Privileged account access is logged and periodically reviewed; • Reports are available on disabled, suspended and in-active users; • Access to the IT solution's audit trail is restricted and controlled; • Access to IT solution's source code is restricted and controlled; and • Access to information systems audit tools is restricted to prevent misuse or compromise e.g. password cracking tools and vulnerability scanning software.	✓	✓	✓
3.2	All IT solutions processing the **Data** must have a configurable system-enforced password and user account policy, which includes:- • Configurable password history; • Configurable maximum password age; • Configurable minimum password age; • Configurable minimum password length (minimum of 8 characters); • Configurable complexity requirements of at least four of the following elements: ○ Numeric – (0-9) ○ Uppercase – (A-Z) ○ Lowercase – (a-z) ○ Special Characters (?,!, @, #, %, etc…) ○ Spaces • Configurable account lockout threshold of invalid logon attempts.	✓	✓	✓
3.3	IT devices accessing the **Data** must have an automated lockout if left unattended or idle for a period of 10 minutes.	✓	✓	X

3.4	System and administrative accounts must have the ability to be changed without resulting in changes to software coding.	✓	✓	✓
3.5	IT Solutions processing the **Data** must have the ability to enable two factor authentication if required.	✓	✓	X
4.	**Expected Control - Network and Infrastructure Security**	**Restricted Data**	**Controlled Data**	**Public Data**
4.1	The Company must hold a current ‘Cyber Essentials Plus’ certification (or equivalent)	✓	X	X
4.2	The Company must hold a current ‘Cyber Essentials’ certification (or equivalent)	X	✓	X
4.3	Networks hosting the **Data** must be held within an authenticated, secure network domain boundary.	✓	✓	✓
4.4	The IT solution must be segregated on networks by the implementation of either physically different networks, or use of logical networks (e.g. virtual private networking), in order to protect the **Data** within the solution.	✓	✓	X
4.5	IT solution(s) and devices hosting/ accessing the **Data** must run up to date anti-virus and malware protection software.	✓	✓	✓
4.6	The IT solution should have the ability to encrypt sensitive data before storage within the database.	✓	✓	X
4.7	Regular backups of the **Data** must be undertaken and encrypted to at least AES 128 standard or equivalent.	✓	✓	X
4.8	Auditing of activities in the **Data** hosting environment must be kept secure and protected against alteration or deletion.	✓	✓	✓
4.9	Intrusion detection strategies must be in place, which include regular penetration testing.	✓	✓	X

4.10	Patch management procedures must be in place to ensure security bug/fixes are applied to all IT solutions hosting the **Data** and are in accordance with the vendors recommended guidance.	✓	✓	✓
4.11	IT devices (including laptops & PCs) used to store or process the **Data** must be protected using whole disk encryption to at least AES 128 standard or equivalent.	✓	✓	X
4.12	Obsolete IT devices used to record, store or process the **Data** must be securely wiped to render the data unrecoverable.	✓	✓	X
4.13	Passwords used to encrypt IT devices and solutions holding the **Data** must meet the following complexity requirements:- • Minimum password length **8** characters; • Include complexity requirements of at least four of the following five elements: ○ Numeric – (0-9) ○ Uppercase – (A-Z) ○ Lowercase – (a-z) ○ Special Characters (?,!, @, #, %, etc…) ○ Spaces	✓	✓	X
4.14	The **Data** must be transferred/exchanged via secure communication channels which are protected by a minimum of TLS v1.2 protocol (or equivalent) that enables as a minimum 256-bit symmetric key encryption using SHA256RSA signature algorithm with RSA public asymmetric key encryption of 2048 bits.	✓	✓	X
4.15	The **Data** must be encrypted to at least AES 128 standard or equivalent, whilst at rest within the hosting environment.	✓	✓	X
5.	**Expected Control - System Acquisition, Development and Maintenance**	**Restricted Data**	**Controlled Data**	**Public Data**
5.1	IT solutions development and maintenance procedures must be in place to ensure information security is an integral part of IT solution development.	✓	✓	X

5.2	Any IT solutions or hardware installed onto the Council's IT infrastructure must be supported by documentation, which details the running environment, installation procedures and any known issues that may adversely affect the security and integrity of the Council's information.	✓	✓	✓
5.3	A separate test environment must be available to replicate the live system to facilitate assessments and development which will not put the Council's IT network at enhanced risk.	✓	✓	X
5.4	'Live' **Data** must not be used in test systems.	✓	✓	X
5.5	The integrity, confidentiality and availability of the **Data** must be maintained during the decommissioning of IT solutions and when moving to a new solution/system.	✓	✓	X
5.6	IT solutions processing the **Data** must have an extractable audit trail which will record 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; and • Details of the user's MAC or IP address (subject to whether the connection is internal or external) of the IT equipment for the user making the connection.	✓	✓	✓
5.7	IT solutions processing the **Data** should have a configurable welcome page to remind users of their obligations when accessing the system.	✓	✓	✓
5.8	To enable continuity of service, procedures should be in place to enable the transfer of **Data** to the Council or new contractor at the end of a contract period.	✓	✓	✓
6	**Expected Control - Business Continuity Management**	**Restricted Data**	**Controlled Data**	**Public Data**
6.1	Procedures must be in place to enable the recovery of IT solutions including user data and/or credentials in the event of interruption to normal operational service.	✓	✓	✓

6.2	Physical and logical access controls must be in place to maintain the security of the **Data** to an equivalent standard to that within the 'live' environment during the business recovery process.	✓	✓	✓
7.	**Expected Control - Expected Controls - Information Security Incident Management and Compliance**	**Restricted Data**	**Controlled Data**	**Public Data**
7.1	An information security management procedure must be in place, including a clear method by which information security incidents are notified to the Council.	✓	✓	✓
7.2	The knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	✓	✓	✓
7.3	Details of information security events/ breaches related to the processing of the **Data**, must be kept secure and protected against alteration or deletion.	✓	✓	✓
7.4	Compliance is required with the following in respect of the **Data**: • General Data Protection Regulations • The Computer Misuse Act (1990); • The Electronic Communications Act (2000); • Privacy and Electronic Communications Regulations (2015); and • The Copyright, Designs and Patents Act (1988).	✓	✓	✓
7.5	Procedures should be in place for third parties to conduct audits of supplier services to ensure that information security, data protection terms and conditions are being adhered to.	✓	X	X

Additional guidance or clarification on the requirements within **Appendix A** can be obtained from the Council's Information Security Team using the following contact details:

Appendix B
Data Protection and Information Security Guidance

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 GDPR 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 an 8 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

Appendix B
Data Protection and Information Security Guidance

PUBLIC

3.	IT equipment and Confidentiality	In Place
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 periodically updated.	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

Additional guidance or clarification on the requirements within **Appendix B** can be obtained from the Council's Information Security Team using the following contact details: