Elizabeth Sloane

DATA MANAGEMENT POLICY

Policy Name	Data Management Policy
Version No	2.0
Contact Person	Data Protection Officer (Grievance Officer): Legal Department
Last Review Date	14th August, 2020
Reviewed By	Nneka Jackson Senior Director Legal & DPO
Approved By	Melanie Wynter, Managing Director

I. Distribution List

Employees and/or Relevant Individuals as defined below of St. Elizabeth Sloane & Company Limited, its subsidiaries, its affiliates in Jamaica (including non-profit organizations and/or trust), hereinafter "**Elizabeth Sloane**".

II. Version History

Version	Date	Description
1.0	23.04.2020	Data Privacy Policy released
2.0	14.08.2020	Amendments to the Policy referring to Elizabeth Sloane's adoption and implementation of the Binding Corporate Rules (BCRs). Amendments reinforcing employee/relevant individual's obligations while handling personal data; And consequences of non-compliance with the Policy.

1. Introduction

St. Elizabeth Sloane & Company Limited (ELIZABETH SLOANE) needs to gather and use certain information about individuals and their company. These can include customers, suppliers, business contacts,employees and other people the organisation has a relationship with or may need to contact. This policy describes how this data must be collected, handled and stored to meet the organisation's data protection standards — and to comply with the law.

2. Purpose

The principles underlying this data protection policy ensures ELIZABETH SLOANE:

- Complies with Data Protection legislation and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach or cyber-attack on its systems.

3. Scope

3.1 This policy applies to all personal data and special categories of personal data (previously known as sensitive data) processed by ELIZABETH SLOANE and as defined underthe General Data Protection Regulation (GDPR), including structured sets of personal data held in electronic or other filing systems that are accessible according to specified criteria.

3.2 'Personal Data' means any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to:

(a) an identifier such as a name, an identification number, location data or anonline identifier; or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

3.3 This can include:

- names of individuals;
- postal addresses;
- email addresses;
- telephone numbers;

- any other information relating to individuals.

3.4 For personal data to be processed lawfully, one or more of the following legal grounds must apply:

- the data subject has given consent to the processing of his or her personaldata for one or more specific purposes;

- processing is necessary for the performance of a contract to which the datasubject is a party or in order to take steps at the request of the data subjectprior to entering into a contract;

- processing is necessary for compliance with a legal/statutory obligation towhich the controller is subject to;

- processing is necessary in order to protect the vital interests of the datasubject or of another natural person;

- processing is necessary for the performance of a task carried out in the publicinterest or in the exercise of official authority vested in the controller;

- processing is necessary for the purposes of the legitimate interests pursued bythe controller or by a third party (although 'legitimate interest cannot generally be used by public bodies as a basis for processing, it is included here in the interest of completeness).

Special categories of personal data (sensitive data)

3.5 These are personal data deemed to be more sensitive by law, and so need additional protection. They cannot be processed unless at least one further condition for processing special category data is fulfilled. These conditions are:

- the data subject has given explicit consent;

- the processing is necessary in the context of employment law, or laws relatingto social security and social protection;

- the processing is necessary to protect vital interests of the data subject or ofanother natural person;

- the processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with itspurposes;

- the processing relates to personal data which have been manifestly madepublic by the data subject;

- the processing is necessary for the establishment, exercise or defence of legalclaims, or for courts acting in their judicial capacity;

- the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursuedand protects the rights of data subjects;

- the processing is required for the purpose of medical treatment undertaken byhealth professionals, including assessing the working capacity of employees and the management of health or social care systems and services;

- the processing is necessary for reasons of public interest in the area of publichealth (e.g. ensuring the safety of medicinal products);

- the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

3.6 Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing. Special categories of data consistof information which relates to:

- the racial or ethnic origin of the data subject;

- their political opinions;

- their religious beliefs or other beliefs of a similar or philosophical nature;

- whether they are a member of a trade union (within the meaning of the TradeUnion and Labour Relations (Consolidation) Act 1992);

- their physical or mental health;

- their sexual life or orientation;

- genetic/biometric data (where processed to uniquely identify an individual).

4. The Policy

4.1 This policy sets out the Department's commitment to: protecting personal data; how this commitment is implemented with regard to the collection and use of personal data; and ensuring the rights of individuals whose data is held (the DataSubject) can be exercised as prescribed by the General Data Protection Regulation. ELIZABETH SLOANE is committed to ensuring that it complies with the underpinningsix data protection principles, as listed below.

4.2 The 6 Data Protection principles:

- personal data shall be processed lawfully, fairly and in a transparent manner inrelation to individuals;

- personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible withthat purpose or those purposes;

- personal data must be adequate, relevant and limited to what is necessary inrelation to the purposes for which they are processed;

- personal data shall be accurate and, where necessary, kept up to date;

- personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, usingappropriate technical or organisational measures.

4.3 These principles will be adhered to with the following ambitions:

- meeting our legal obligations as laid down by the GDPR;

- ensuring that data is collected and used fairly, lawfully and transparently (excepting the provisions of the Law Enforcement Directive);

- processing personal data where an appropriate legal basis to do so exists andonly in order to meet our operational needs or fulfil legal requirements;aking steps to ensure that personal data is up to date and accurate;

- establishing appropriate retention periods for personal data;

- ensuring that data subjects' rights can be appropriately exercised;

- ensuring that a nominated officer is responsible for data protection complianceand provides a point of contact for all data protection issues, i.e. Data Protection Officer;

- ensuring that all staff are made aware of good practice in data protection;

- providing adequate training for all staff responsible for personal data;

- ensuring that everyone handling personal data knows where to find further guidance;

- ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;

- sharing information where required by law and where approved information sharing agreements are in place and when agreed processes have been followed;

- regularly reviewing data protection procedures and guidelines within the organisation;

- adopting local and national data protection best practice, including incorporation of appropriate learning from any published ICO data protectionand/or European Data Protection Board (EDPB) guidance;

- publishing and promoting this policy and the rights of data subjects includinghow to make a right of access request;

- registering with the Information Commissioner as an organisation which handles data;

- establishing procedures for reporting data protection breaches to relevant authorities for investigation, including self-referral mechanisms;

- being clear with individuals whose data we process as to how we store it, whatwe do with it and why;

- responding to any valid subject access requests promptly and in any eventwithin one month of receiving them (unless limited exceptions apply).

5. Data Protection Risks

5.1 This policy helps to protect ELIZABETH SLOANE from some very real data security risks,including:

- breach of confidentiality and public trust; for instance, information being shared inappropriately;

- failing to offer choice; for instance, all individuals should be free to choose howthe organisation uses data relating to them when the processing is by consent;

- failing to observe the enhanced rights that citizens have under the GDPR - for example, right of access, right to rectification, etc;

- reputational damage; for instance, the Department could suffer if hackers wereto successfully corrupt, gain access to or steal sensitive data.

6. Roles and Responsibilities

6.1 ELIZABETH SLOANE's responsibilities:

- ELIZABETH SLOANE is the data controller under Data Protection Legislation for the personaldata it processes for its own purposes.

- the Accounting Officer has overall responsibilities for compliance with data Protection legislation;

- the ELIZABETH SLOANE Data Protection Officer (DPO) is responsible for monitoring progress and advising the organisation on implementation of this policy; actingas primary contact on any data protection queries; and approving responses to Right of Access requests (generally described in this document as 'Subject Access Requests');

- the DPO is also responsible for monitoring the completion of all mandatory training for all staff (with special emphasis on staff handling personal data ondaily basis) and to ensure access to further guidance and support;

- ELIZABETH SLOANE provides clear lines of reporting and an appropriate separation of dutiesto allow the DPO to supervise compliance with GDPR, reporting to board level;

- the DPO will conduct regular assurance activity to monitor and assess new processing of personal data;

- the DPO will monitor and report on all data processor requirements e.g. Roles& Responsibilities, notification, data subject access requests;

- the DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (employees, customers etc.).

Employee responsibilities

6.2 All employees have individual responsibility for complying with this policy and following accompanying guidance.

6.3 All employees will undertake relevant data protection training, including the Civil Service Learning ‘Responsible for Information’ training, and any other training thatshall be deemed as mandatory.

6.4 Employees will:

- observe all forms of guidance, codes of practice and procedures about the collection, sharing, handling and use of personal information;

- develop a comprehensive understanding of the purpose for which ELIZABETH SLOANE usespersonal information;

- collect and process information in accordance with the purpose for which it is required to be used by ELIZABETH SLOANE to meet its statutory requirements and businessneeds;

- ensure the information is destroyed when no longer required in line with our information management guidance.

- upon receipt of a request by or on behalf of an individual for information held about them (Subject Access Request), staff will refer requests to the Information and Security Compliance Team as quickly as possible so that therequest can be acted on quickly and legal advice sought if required.

- understand that breaches of this policy may result in scrutiny by the Information Commissioner’s Office (ICO) with the potential for fines to be levied and accompanying reputational damage. There is also the potential formisconduct action.

7. Data Protection ImpactAssessments

7.1 A Data Protection Impact Assessment (DPIA) will be carried out if a project or the introduction of a new service or policy is likely to result in a high risk to the privacyof individuals. A DPIA is a process that helps identify privacy risks and ensure lawful practice when a new project is designed, or changes are made to an existing service or policy.

7.2 The purpose of the DPIA is to ensure that privacy risks are mitigated including promptly addressing any identified issue while allowing the aims of the project orpolicy to be met whenever possible.

7.3 According to the Information Commissioner's Office, a DPIA is required when an organisation plans to:

- embark on a new project involving the use of personal data;

- introduce new IT systems for storing and accessing personal information;
- participate in a new data-sharing initiative with other organisations;
- use profiling or special category data to decide on access to services;
- initiate actions based on a policy of identifying particular demographics;
- use existing data for a new and unexpected or more intrusive purpose;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providingthem with a privacy notice (‘invisible processing’);
- profile children or target services at them; or
- process data that might endanger the individual’s physical health or safety inthe event of a security breach;
- continue to utilise long standing databases where the DPIA may not havebeen considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues.

7.4 Guidance issued by the Information Commissioner's Office on DPIAs can be foundon the ICO website.

8. Data Protection by Design and Default

8.1 In compliance with data protection by design principle, we will ensure data protection risks are taken into account throughout the process of designing a new process, product, policy or services, rather than treating it as an afterthought. Thismeans assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processingcomplies with the law and protects the rights of the data subjects.

8.2 To comply with data protection by design and by default principles, we will ensure mechanisms are in place within the organisation to ensure that, by default, only personal data which are necessary for each specific purpose are processed. Thisobligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limitedto that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

9. Breach Notification and Reporting

9.1 We must report any losses or suspected breaches of personal data to the Information Commissioner within 72 hours of becoming aware of the breach.

9.2 When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we are required by law to notify the affected individuals without undue delay.

9.3 If you discover or suspect a breach of data protection rule, loss or compromising of personal data, you must report it immediately to the Information and Security Compliance Team at tech@elizabethsloane.com. The data breach reporting form is included as an annex at the end of this policy document.

10. General Staff Guidelines

10.1 The only people able to access data covered by this policy should be those whoneed it for their work.

10.2 Personal data should not be shared without adherence to relevant guidance. When access to confidential information is required, employees can request it fromtheir line managers.

10.3 ELIZABETH SLOANE will provide training to all employees to help them understand theirresponsibilities when handling data.

10.4 Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

10.5 Strong passwords must be used, and they should never be shared.

10.6 Personal data should, under no circumstances, be disclosed to unauthorised individuals, either within the department or externally.

10.7 Data should be regularly reviewed and updated if it is found to be out of date. If nolonger required, it should be deleted and disposed of.

10.8 Employees should request help from their line manager or the Data ProtectionOfficer if they are unsure about any aspect of Data Protection.

11. Data Storage

11.1 This policy document describes how and where data should be safely stored.When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see/access it.

11.2 These guidelines also apply to data that is usually stored electronically but hasbeen printed out for some reason:

- when not required, sensitive paper or files should be kept in a locked drawer,for filing cabinet;

- employees should make sure sensitive paper and printouts are not left where unauthorised people could see them, for example on a printer or unattended on a desktop:

- sensitive data printouts should be shredded and disposed of securely when nolonger required;

- all ELIZABETH SLOANE information should be handled in line with the acceptable use of our Policy

11.3 When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:

- data should be protected by strong passwords that are changed regularly andnever shared.

- if data is stored on removable media (e.g. CDs or data sticks), these should bekept locked away securely when not being used.

- data should only be stored on designated drives and servers and should onlybe uploaded to an approved cloud computing service.

- servers containing personal data should be sited in a secure location, awayfrom general office space.

- data should be backed up frequently. Those backups should be regularlytested.

- ELIZABETH SLOANE Data should under no circumstances be saved directly to personallaptops or other mobile devices such as tablets or smart phones.

12. Data Use

12.1 Personal data is of no value to ELIZABETH SLOANE unless the business can make use of it.However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- when working with personal data, employees should ensure their computersare always locked when left unattended;

- personal data should not be shared informally. In particular, it should never besent by non-compliant webmail, as this form of communication is not secure;

- personal data must be encrypted before being transferred electronically outside of those email domains approved within the Acceptable Use of ICT policy. The IT department can explain how to send data to authorized external contacts.

- personal data should not be transferred outside of the European Economic Area except where appropriate safeguards have been put in place or the country or territory ensures an adequate level of protection for the rights andfreedoms of data subjects in relation to the processing of personal data. If there are any queries about this, please contact the Information and Security Compliance Team;

- employees should under no circumstances save copies of personal data to their own computers. Such data should always be accessed and updated viaapproved IT equipment.

13. Data Accuracy

13.1 The law requires ELIZABETH SLOANE to take reasonable steps to ensure data is kept accurateand up to date. It is incumbent upon ELIZABETH SLOANE to ensure personal data held and processed is accurate and to ensure it continues to be accurate. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

13.2 Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

13.3 Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer’s details when they call.

13.4 ELIZABETH SLOANE will make it easy for data subjects to update the information ELIZABETH SLOANE holds about them.

13.5 Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should beremoved from the database

13.6 Where additional data sets are required the Information and Security ComplianceTeam should be engaged to ensure this is reflected on the Department's Information Asset Register.

14. Right of Access Request / SubjectAccess Request

14.1 All individuals who are the subject of personal data held by ELIZABETH SLOANE are entitled to:

- ask what information the organisation holds about them, how it is used and why;
- ask how to gain access to it;
- be informed how to keep it up to date;
- be informed how the organisation is meeting its data protection obligations.

14.2 A request for access to personal information held by ELIZABETH SLOANE (known as Right of Access Request or a Subject Access Request) must be responded to within one calendar month.

15. Providing Information

15.1 ELIZABETH SLOANE aims to ensure that individuals are aware that their data is being processed,and that they understand:

- how the data is being used;
- who it is shared with;
- how long it is kept for;
- how to exercise their rights.

15.2 To these ends, the Department has a privacy statement; setting out how datarelating to individuals is used by the organisation.

16. Monitoring, Review and Evaluation

16.1 The Management Committee will monitor the Department's approach to data protection and associated rights.

16.2 This policy will be reconsidered against any legislative changes and reviewed onan annual basis.

17. Access Control Policy

Principle of Least Privilege

Access controls must be allocated on the basis of business need and ‘Least Privilege’. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfiltheir business role.

User Access Account Management

User account management procedures must be implemented for user registration,modification and de-registration on all Elizabeth Sloane information systems.

These procedures must also include processes for monitoring redundant andinactive accounts.

All additions, deletions, suspensions and modifications to user accesses should becaptured in an audit log showing who took the action and when.

These procedures shall be implemented only by suitably trained and authorizedemployees.

Access control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks yetallows the organisation’s business activities to be carried out without undue hindrance.

A review period will be determined for each information system and access controlstandards will be reviewed regularly at those intervals.

All access to Elizabeth Sloane information systems must be controlled by an approvedauthentication method supporting a minimum of a user ID and password combination that provides verification of the user’s identity.

Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policymust be authorised by the Senior Responsible Owner (SRO) or, where applicable, the Authority.

All users shall have a user ID for their sole use for access to all computingservices. All individual user IDs must be unique for each user and never duplicated.

All user accounts that have not been accessed for an agreed period, without priorarrangement, must be automatically disabled.

All administrator and privileged user accounts must be based upon job functionand authorised by the SRO or, where applicable, the Authority, prior to access being given.

All changes to privileged accounts must be logged and regularly reviewed.

Procedures shall be established for all information systems to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever thereis a change in business need, a user changes their role, or a user leaves the organisation.

Users’ access rights will be reviewed at regular intervals no longer than annually.

Access to systems by individual users must be authorized by their manager orwhere applicable, the Authority.

Password Management

Passwords must not be shared with any other person for any reason.

All default system and vendor passwords must be changed immediately followinginstallation.

All Elizabeth Sloane information systems must support strong password managementtechniques (such as: length, complexity, aging, history, account lockout).

All Elizabeth Sloane information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter on a regularbasis.

Monitoring User Access

Systems will be capable of logging events that have relevance to potentialbreaches of security.

User access will be subject to management checks.

Responsibilities

Senior Responsible Owner (SRO)

SROs are responsible for ensuring that the requirements of this policy are implemented within any programme, projects, systems or services for which theyare responsible.

The SRO is responsible for ensuring that a robust checking regime is in place andcomplied with to ensure that legitimate user access is not abused.

The SRO may delegate responsibility for the implementation of the policy butretains ultimate accountability for the policy and associated checking regime.

Any non-compliance with this policy must be supported by a documented andevidence based risk decision accepted by the SRO.

Managers

Managers are responsible for ensuring that members of their team have theminimum levels of access to systems they need to perform their job.

They must authorise the access rights for each individual team member and keepa record of the latest access permissions authorised.

Managers should ensure that the access rights of people who have a change of duties or job roles or left the organisation are revoked immediately and that any access tokens (smartcard/USB dongle) are recovered.

All Managers should review the access levels of their people to ensure they are appropriate.

IT Support Teams

IT Support Teams are responsible for granting access to systems as described in local work instructions or use of Role Based Access Controls Matrix in accordancewith the relevant procedures.

IT Support Teams must evaluate and, if necessary, challenge authorised access to help identify any obvious anomalies in the access levels granted or requested.

Users

Users must only use business systems for legitimate use as required by their joband in accordance with the procedures for those systems.

Compliance

Compliance against this policy will be assessed regularly.

Any violation of this policy must be investigated and may result in disciplinaryaction being taken.

18. Information and ICT Incident Management

1 Introduction

1.1 The purpose of this Policy is to ensure that information security events and weaknesses associated with information systems and hard copy documentation are communicated in a way that allows timely, corrective action to be taken, so that the Council's information and data is protected from any actual, suspected or potential security events.

1.2 The definition of an incident is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and/or personnel.

1.3 Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

1.4 An information security event or weakness can also arise through loss, misuse or compromise of hard copy information or data and this policy equally applies to such losses.

2 Policy Statement

2.1 The purpose of this Policy is to ensure that any incidents that affect the daily operations are managed through an established process.

2.2 All Employees have an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

2.3 This Policy provides a framework for reporting and managing:

- Security incidents affecting the Council's information and ICT systems
- Losses of information
- Near misses and information security concerns

3 Scope

3.1 This Policy applies to all Employees and third parties working for or on behalf of the Council with any form of access to a Council computer device or ICT system. For the purpose of this Policy the term 'Employee' refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

3.2 This Policy should be read in conjunction with the Code of Conduct, the Council Comprehensive Equality Policy and other associated relevant policies, procedures and guidance as contained within the Information Management Framework.

4 Security Incidents and Weaknesses

4.1 An Information Security Incident can be described as an event that results in:

- The disclosure of confidential information to an unauthorised individual.
- The integrity of a system or information being put at risk.
- The availability of a system or information being put at risk.

4.2 Initially, there are four categories: events, weaknesses, incidents and unknowns:

- Events – Occurrences that, after analysis, have no or very minor importance for information security.
- Vulnerabilities – Weaknesses that, after analysis, clearly exist as significantweaknesses compromising information security.
- Incidents – Occurrences of events (series of events) that have a significant probability of compromising the Council's information security.
- Unknowns – Reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.

4.3 A weakness is the potential for an incident to occur.

Incidents and Weaknesses to Report

4.4 Information security events and weaknesses need to be reported at the earliest possible stage. It is vital that as much information is gained as possible to identify whether reported events or weaknesses are security incidents and to determine any further cause of action.

4.5 Actions to fix any damage caused by an Incident must be put through Business IT change management process. Any actions should be aimed at fixing the cause and preventing re-occurrence.

4.6 Security events and weakness that must be reported include:

- Theft or loss of equipment, data or information (including removable media)
- Breaches of physical security arrangements
- Computer infected by a virus or other malware
- Receiving unsolicited mail of an offensive nature or requesting personal data
- Unauthorised disclosure of information including information being faxed, emailed,posted or handed to an unintended recipient
- System malfunctions which may compromise security
- Inadequate disposal of confidential material
- Writing down passwords and leaving them on display or somewhere easy to find
- Non-compliance with policies or guidelines
- Accessing an individual's record inappropriately
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Accessing a computer database using another Employee's credentials (User ID and password), either with or without their authorisation.

(Please note this list is not exhaustive)

4.7 Employees must not attempt to prove/exploit a security weakness as such an action may be misuse.

4.8 Employees must not attempt to investigate a suspected security breach as such action may compromise any investigation.

5 Reporting Procedure

5.1 All information and ICT security events and weaknesses must first be reported to an individual’s Line Manager. In the absence of the individual’s Line Manager, the Departmental Information Management Group (IMG) Representative must be informed.

5.2 All events and weaknesses must be reported at the earliest opportunity to the IT Service Desk.

5.3 If applicable, you must note the symptoms and any error messages on screen and await further instructions from a member of IT.

6 Management of Incidents

6.1 A consistent approach to dealing with all information security events must be maintained across the Council.

6.2 Business IT will investigate all IT related information security events and weaknesses. The System & Information Management Officer (SIMO) will investigate incidents resulting in the loss, misuse or compromise of personal data (whether real or potential). Information Security Incidents will be reported to the IT Policy & Regulation Group for review.

6.3 Where an information security event is considered to fall within the notification guidelines issued by the Information Commissioner’s Office (ICO), the IMG Representative, in agreement with the Data Protection Officer, will prepare the necessary notification and deal with all correspondence arising from it.

Collection of Evidence

6.4 If an incident requires information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care.

6.5 For further guidance see the Forensic Readiness and Investigation Policy.

6.6 For other incidents, including loss or compromise of hard copy information, as much information as possible on the circumstances of the incident must be collated in order to assist the SIMO to investigate.

7 Responsibilities

Information Management Group (IMG)

7.1 The role of the IMG is to co-ordinate the approach to every aspect of Information Management, and not just compliance with DPA 1998.

7.2 The group is made up of Departmental Information Management Representatives who are senior managers in each Department and are responsible for a multi-disciplinary approach to the management of information throughout their Departments.

7.3 The IMG is responsible for the overarching governance and implementation of the Policy throughout the Council.

7.4 The IMG is responsible for ensuring that all Employees are fully aware of Council policy andprocess, and have received appropriate training.

7.5 The IMG is also responsible for the development and monitoring of the adherence to the Policy.

7.6 IMG Representatives are responsible for ensuring any security information incidents reported to them are referred to the IT Service Desk.

7.7 IMG Representatives have a duty to ensure their Department/Service area cooperates fully with Business IT and/or the SIMO with any investigations.

7.8

IT Policy & Regulation Group

7.9 The IT Policy & Regulation Group (ITPARG) will review all incidents reported to it and advise on any further action required.

7.10 ITPARG will action any lessons learned from reported incidents/weaknesses to prevent future incidents, this will be recorded within their minutes.

7.11 Where necessary, as part of the review of reported incidents/weaknesses ITPARG may re-classify the event.

7.12

Business IT

7.13 Business IT will investigate all ICT security incidents.

7.14 The Incident Management Procedure or Major Incident Management Procedure (if appropriate) must be followed. IT Support Staff will not be expected to take specific action over events or weaknesses that arise in relation to hard copy documentation.

7.15 All Employees involved in incident management will have access to relevant information such as known errors, problem resolutions and the configuration management database (CMDB).

7.16 The reporting Employee must be kept informed of the progress of their reported incident.

7.17 The Service must be alerted in advance if their service levels cannot be met and an action agreed.

7.18 Incidents that are considered service affecting must be reported to the relevant Service Manager and System Owner, in order to make the necessary Business Continuity arrangements.

7.19 Incidents should be promptly reported to Internal Audit for information purposes.

7.20 Business IT will present a summary report on ICT security incidents to the IT Policy and Regulation Group.

System & Information Management Officer (SIMO)

7.21 When an information security event or weakness is reported which could potentially involve personal data the SIMO will co-ordinate the investigation alongside the relevant Line Manager or, where appropriate, conduct an investigation

7.22 The SIMO will provide advice and recommendations, where necessary, on actions to be taken following potential/actual data breaches.

7.23 All incidents will be reported to the IMG.

Line Managers

7.24 Line Managers are responsible for ensuring all Employees in their Service area adhere to the Policy.

7.25 Line Managers must report any security event or weakness to the IT Service Desk.

7.26 Where Line Managers conduct an investigation, all outcomes must be reported to the SIMO.

Employees

7.27 Employees must report any security event or weakness at the earliest opportunity to their Line Manager or the IT Service Desk.

7.28 Relevant Employees connected to an incident will be required to supply any necessary information which will help in establishing the events which led to the incident occurring.

7.29 All Employees must cooperate fully with Business IT and/or the SIMO during any investigation. Employees may be interviewed as part of this process.

8 Review and Governance

Policy Governance

8.1 The Policy will be subject to governance through the IMG, and will be formally approved Executive Decision Framework.

8.2 The Policy will be subject to at least an annual review, and where changes in legislation require, more frequent.

9 Policy Compliance

9.1 If you are found to have breached this Policy, the matter will be considered and investigated under the Council's disciplinary procedure.

9.2 Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

ANNEX - Data Breach Reporting Form

Details:
Date;
Time;
Location of the incident.	

Type of Breach involved and sensitivity (see Annex B)	
Is there Breach of personal information?	
If yes, number of individuals or records that maybe at risk. Is there potential for financial harm?	
Has: the individuals concerned have been informed;a decision has been taken not to inform; this has not yet been decided. (The Informationand Security Team should be asked for advice before the individuals concerned are informed)	
What incident management procedures are being followed and what disciplinary action willbe invoked?	
Description of what happened (including whetherit was a theft, accidental loss, inappropriate disclosure, procedural failure) or unauthorised disclosures.	
How the information was held? paper, memory stick, disc, laptop (digital/paper), tablets or smart phones.	
If digital format, was it encrypted?	
Whether the media (press etc.) is involved or isthere a potential for media interest?	
Are there any legal implications?	

Who has been informed? WTD- Information and Security team[1] Senior Information Risk Owner Chief Executive Accounting Officer Caldicott Guardian Police, Counter Fraud Branch, etc.	