eastsussex.gov.uk

East Sussex
County Council

Data Protection and Information Security Policy

V3.0

Target Audience:	ESCC Staff, members and other agencies handling ESCC information
Policy Endorsed by:	Information Strategy Board

INVESTORS IN PEOPLE

POSITIVE ABOUT DISABLED PEOPLE

Data Protection & Information Security Policy

Summary

This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when handling personal information within ESCC.

Contents

Data Protection & Information Security Policy

1. Introduction

The objective of the Data Protection & Information Security Policy is to ensure that confidential information used to deliver our services is treated with appropriate security by all who handle it. 'Appropriate' is a degree of precaution and security proportionate to the potential risk and impact of loss or accidental disclosure.

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore anyone handling personal information MUST take personal responsibility and make considered judgements in terms of how they handle this information whilst delivering their service. If in any doubt they should seek clarification from their line manager, their Information Governance Officer, Information Security Team or the Data Protection Officer.

Overall impact is determined by the degree of sensitivity of the information and the quantity involved, but you must remember that a single record about an individual can have a potentially significant impact on that individual if accidentally disclosed to others.

2. Policy statement

It is the policy of East Sussex County Council (the Council) that:

- we will protect information from a loss of:
  - confidentiality (ensuring that information is accessible only to authorised individuals)
  - integrity (safeguarding the accuracy and completeness of information)
  - availability (ensuring that authorised users have access to relevant information when required)
  - relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff
- we will report and follow-up all breaches of information security, actual or suspected

Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information.

3. Scope and application

The Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees and elected members, it also applies to volunteers, work experience candidates, and all staff of service delivery partners and other agencies who handle information for which the Council is responsible. It will form the basis of contractual responsibilities as set out in the mandatory contract clauses where reference is made to the Council's Data Protection and Information Security Policy.

4. The legal basis

The Council must comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001
- Health and Safety at Work Act 1974

The requirement to comply with this legislation extends to everyone as set out at 3.2 above who are held personally accountable for any breaches of information security for which the Council is responsible.

5. Definitions

Information and data

Information results from the acquisition and collation of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper, fiche) phone calls and conversations. For the purpose of this policy information and data can be regarded as the being the same.

Information/Data Types

This policy relates primarily to any information that would be classified as Official Sensitive (Personal) i.e. data relating to individuals/Personally Identifiable Information (PII). Information classified as Official Sensitive (Commercial) should also be handled in accordance with this policy where applicable. Official Sensitive information should by default be treated as confidential.

- Personally Identifiable Information (PII) - any information relating to an individual (‘data subject) who can be identified directly or indirectly by an identifier such as name, ID number, location data (e.g. address), online identifier (e.g. IP address) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

- Special Category Data - sensitive personal data (which requires extra protection) including any information that may identify an individual's:
    - racial or ethnic origin,
    - political opinions,
    - religious or philosophical beliefs,
    - trade union membership,
    - health,
    - sex life/orientation
    - genetic/biometric identifier
    - criminal convictions

Information that is confidential but doesn't relate to an individual or individuals (Official Sensitive (Commercial)) includes the following:

- Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings

An easy sense check on whether information is personal or commercially confidential is:

- Is the information covered by Data Protection Legislation or any further duty of confidence?
- Could release of the information cause problems or damage to individuals, the public, the Council or a partner organisation? This could be personal, financial, reputation or legal damage
- Could release of the information prejudice the outcome of negotiations or investigations?

If in doubt seek advice from line management or relevant Information Governance or Security Officer and err on the side of caution, treating the information as sensitive and confidential.

6. Governance and accountabilities

The **Senior Information Risk Owner** (SIRO) is the Chief Operating Officer and is the focus for the management of information security at CMT level and will approve appointments and resources required to support policy and procedures. The SIRO will ensure that policy and resources are integrated into Council processes appropriately and within the business context.

The **Information Strategy Board** is chaired by the SIRO and responsible for ensuring compliance with information security policy, protocol, law, regulation and guidance.

Directors are responsible for ensuring that all employees, contractors and partner organisations with legitimate access to information held on the Council's behalf within their department are familiar and compliant with their responsibilities under Data Protection legislation, the Freedom of Information Act 2000 and other relevant legislation as well as the relevant policies and standards of the Council.

The corporate **Information Governance Steering Group (IGSG)** will develop policies and strategic plans in support of data protection and information security and work together across departments, with external agencies and service delivery partners, to ensure that compliance with policy is maintained.

The corporate **Data Protection Officer** is responsible for co-ordinating all Data Protection activities within the Council, helping and advising departments, monitoring compliance with legislation and acting as the point of contact with the Information Commissioner's Office.

The Customer Services Team is responsible for co-ordinating all Freedom of Information activities with the Council, helping and advising departments and monitoring compliance with legislation.

The **Caldicott Guardian** (Adult Social Care and Children's Services departments only) will oversee disclosures of individual personal information with particular attention being paid to extraordinary disclosures (those which are not routine) in accordance with the relevant *Confidentiality Code of Practice*.

Departmental **Information Asset Owners** will contribute to risk management and understand information assets and assist in monitoring the Council's Information Asset Register so that risks can be assessed and appropriate controls applied.

Departmental **Information Governance Officers** are responsible for providing advice and guidance, ensuring corporate requirements are met and all relevant aspects of the legislation are complied with.

Departmental **Information Governance/Security Officers** are responsible for coordinating investigations of information security incidents and breach management within their departments.

The corporate **IG Lead** is responsible for provision of advice and guidance in relation to information security and maintaining a central log of information security incidents.

All **managers** are directly responsible for implementing procedures and standards within their business areas to maintain compliance with policy.

7. Management of Information

The Council will manage information in accordance with the principles and procedures within this policy and annex and relevant departmental policies and standards.

It is important that the public and our partners have confidence in our ability to handle sensitive and confidential information appropriately. The following principles apply:

- All identifiable personal information is to be treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- All departments will maintain procedures to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information must be recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

8. Creation of records

The Council will create and maintain adequate records to meet the Council's business needs and to account fully and transparently for all actions and decisions. Such records should provide credible and authoritative evidence; protect legal and other rights of the Council, its staff and those who have dealings with the Council; facilitate audit; and fulfil the Council's legal and statutory obligations.

9. Access to Records

Information will be made available on request to anyone who has a right to see it under relevant legislation such as Data Protection or Freedom of Information.

10. Openness and Transparency

Information will be made accessible:

- to anyone, in ways that suit their needs and engenders public trust and confidence in the Council's operations and in compliance with Data Protection and Freedom of Information legislation
- to Council staff where it is necessary for the delivery of their services and the discharge of their duties
- to our partners, where it is lawful and necessary for the delivery of joint services and in the interests of our community and in accordance with agreed information sharing protocols.

11. Information Sharing

Official Sensitive information will be shared with other organisations only where there is a need or obligation to do so and always only where there is a lawful basis to do so. The Council will also share information as required by law.

12. Records Management

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the ESCC Records Management and ESCC Electronic Records Management policies.

13. Data Quality and Assurance

The Council will ensure that information is accurate at the time of capture and will be subsequently maintained to ensure accuracy, integrity and consistency across systems.

14. Handling sensitive or confidential information

Information and the underlying data have a lifecycle covering creation/acquisition, maintenance and use, disclosure, storage and disposal. Annex A sets out the *minimum* standards for handling confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

Due to the particular sensitivity of the information and the nature of the service in Adult Social Care and Children's Services all staff in these departments must adhere to any specific policies, standards and procedures set out for their service areas in addition to the minimum standards set out in Annex A.

15. Information Systems Acquisition, Development and Maintenance

The Chief Information Officer will ensure that all new information systems, applications and networks include a risk assessment and remedial actions as necessary.

System owners will develop and maintain system operating procedures for systems under their control to ensure compliance with this policy.

16. Technical Compliance

The Chief Information Officer is to ensure that information systems are checked regularly for technical compliance with relevant security implementation standards including:

- Government Connect Code of Connection (PSN) or equivalent
- Data Security and Protection Toolkit
- Payment Card Industry Data Security Standard (PCIDSS)

Operational systems will be subject to technical examination to ensure that hardware and software controls have been correctly implemented.

17. Business Continuity

The Council's business continuity planning process will include consideration of information security gained from the information asset and risk register.

18. Risk Management

Risk management will be conducted to register information assets, assess the risks to those assets, evaluate the impact of those risks and control, modify or mitigate against the risks. Overall responsibility will rest with the SIRO who will direct risk management. Chief

Officers will retain the discretion to exercise local risk management commensurate with their particular business needs.

The plan will be implemented by:

- Maintaining a corporate asset register
- Conducting risk assessment
- Applying risk mitigation in context with business demands
- Measuring results and improving the process from lessons learned
- Implementing training and awareness programmes
- Implementing procedures for the detection and control of security events and incidents

19. Quality Assurance and Audit

The Information Security policy, standards and procedures will be audited periodically as part of the annual Internal Audit work plan.

20. Culture and Awareness

This policy is supported by a positive information security culture programme running through the Council. The Information Strategy Board via the Information Governance Steering Group will consider and recommend initiatives to CMT to promote and maintain positive awareness.

21. External Assurance

We will promote to all of our residents, customers, third parties and partners our commitment to information security. The Information Governance Steering Group will provide this assurance on a regular basis.

22. Employees

Pre-employment checks on candidates we are going to appoint for employment and contracts will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements. Guidance is available on the staff intranet and Czone.

Information Security will be included in job descriptions and person specifications as appropriate. Personal objectives and training for employees will be agreed as part of the appraisal process and will include the practice and encouragement of Information Security.

All new employees will undergo e-learning induction in Information Security, Data Protection and Freedom of Information, covering the principles and legal aspects. Subsequently, all employees will undertake further or refresher training as required to maintain safe access to sensitive and confidential information.

23. Partners and Third Parties

Chief Officers will ensure that contractors, partners and third parties agree to terms and conditions consistent with Council policy. Access to and handling of Council information will be managed through departmental procurement and partnership arrangements and subject to appropriate agreements and monitoring, including site visits where necessary and practicable.

Chief Officers will also report any known security breaches by partners and third parties, even if the breach does not involve the Council, in order to monitor their general security standards.

24. Handling Information Security Incidents

Any loss of confidential information, either actual or suspected, must be reported immediately to the relevant line manager or theirs if they are not available. See the Information Security Incident Reporting Policy.

A clear process you must follow is set out in the Information Security Incident Reporting Procedure. The incident will be handled in the first instance by the line manager and department Information Governance/Security Officer who will notify other parties as required by the procedure.

25. Breaches of policy

Where Council members, employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.

However, if Council members, employees or service delivery partners are found to be in breach of the policy and its guidance then they may be subject to disciplinary or other appropriate action.

Information Security Policy - Annex A

Standards for handling confidential information

The following standards are set out for all members, employees and service delivery partners as the *minimum* standards for handling sensitive and confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

Due to the particular sensitivity of the information and the nature of the service in Adult Social Care and Children's Services all staff in these departments must adhere to any specific policies, standards and procedures set out for their service areas in addition to the minimum standards set out in Annex A.

A.1 Creation/acquisition

When information is acquired and records created there are some simple principles you must follow:

You must ensure that it is:

- accurate (factual or qualified expert opinion)
- up to date (changes updated as soon as possible)
- consistent (the same information across different datasets)
- relevant (only as much and for as long as needed for the intended purpose)

When acquiring and handling personal information you must comply with the processes and standards set out under Data Protection legislation.

A.2 Maintenance and use

Information and records must be maintained to ensure that they are accurate, up to date and consistent. When using confidential information there are some ground rules you must follow to maintain confidentiality and integrity:

- never leave the information where others could see it e.g. on a desk, computer screen or left on a fax or printer
- do not discuss the information where others not authorised may overhear
- only use the information for the purpose for which it was collected
- changes must be recorded as soon as possible after the change occurs
- always store information securely, following filing procedures in structured file systems
- always put the information/records back as soon as you have finished using them

- do not produce copies unless they are needed and always update the master record, securely destroying copies as soon as they are no longer needed
- review the information regularly to ensure it is accurate and up-to-date
- if information and records are taken from a secure location the risk of loss increases and you must follow the standards set out in the Data in Transit policy

A.3 Disclosure

Prior to disclosure of personal or commercially confidential information you should be satisfied that at least one of the following applies:

- for personal data, requirements of Data Protection legislation are satisfied (see Data Protection – Guidance for Employees)
- disclosure is permitted under an exemption set out in Data Protection legislation; (e.g. the prevention or detection of crime, the capture or prosecution of offenders, and the assessment or collection of tax or duty)
- disclosure is in the public interest, (e.g. for safeguarding national security or for preventing harm to children or adults)

You must never disclose confidential information to anyone who does not have a right to see it.

If you are unsure do not disclose the information. Seek advice from your manager, departmental Information Governance or Information Security lead or Data Protection Officer.

A.4 Storage

All confidential information must be stored securely and access allowed only to those who need it for legitimate purposes.

Secure storage can be secure buildings with access controls to the building, specific floors and individual offices. The controls can be swipe cards, keypads, key locks etc. Appropriate measures must be used depending on the sensitivity of the information and who should have access to it.

Similarly access to electronic information must be controlled by the use of passwords and assigned permissions within the systems that hold the information.

To ensure appropriate access under these controls you MUST NOT let others use your access whether it is a swipe card, key, login or system password or other access control.

A.5 Disposal

When disposing of any sensitive and confidential information you must comply with the Council's Retention and Disposal Schedules for the specific information and records being disposed.

When disposing of confidential information you must always use secure methods such as cross-cut shredding or pulping or the confidential waste bins where available and keep the waste in a secure place until it can be collected for secure disposal. NEVER put sensitive and confidential waste in normal waste bins.