Information Security Document

Corporate Data Protection Policy

Version 4.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	26/11/2017	First Draft for consideration by IGG	Simon Hobbs
2.0	08/01/2018	Approved by Information Governance Group.	Simon Hobbs
3.0	14/05/2018	Revised Draft to take account of GDPR requirements and to incorporate Article 30 Record of Processing and Schedule 1 Part 4 of the Act relating to an appropriate policy document and safeguards	Simon Hobbs
4.0	04/02/2019	Reviewed by Information Governance Group. EU changed to EEC.	Simon Hobbs

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and Protection of personally identifiable information

Everyone at Derbyshire County Council has an important role to play in ensuring that personal information is processed lawfully and fairly. Personal information is information relating to a living individual who can be identified. We hold personal information about all sorts of people we deal with, as detailed in the Registers identified below, including employees and Members.

All personal information must be dealt with properly no matter how it is collected, recorded and used, whether on paper, in a computer, or on other material. This is not just policy and good practice: it is the law – the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

http://ec.europa.eu/info/law/law-topic/data-protection_en.pdf

Every employee and Member has a duty to be aware of the Acts' principles and this policy in order to ensure that the Council complies with the law on data protection. IG Training is accordingly compulsory for all staff.

The law is there to protect people's personal data; it should not be seen as a hindrance to the Council's operations.

Data Protection Principles

To meet the requirements of the Data Protection Act 2018, Derbyshire County Council **fully endorses the six principles stated therein, and all employees and Members must adhere to them at all times.**

These principles are as follows.

Personal Data must be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and, where necessary, kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary[1];

f) 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.

[1] There is an exception for archiving. Archiving here means offering records of historical interest to the Derbyshire Record Office whose staff will ensure that the records are managed in accordance with GDPR

Derbyshire County Council's Commitment to the Data Protection Principles

Derbyshire County Council will:

- Observe fully the conditions regarding the fair collection and use of information including obtaining fair consent if this is required
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, but only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply checks on the time that information is held to ensure that it is erased at the appropriate time
- Ensure that the rights of people about whom we hold information are able to be exercised in accordance with the GDPR and the 2018 Act, including
  – the right to be informed that processing is being undertaken
  – the right of access to their personal information
  – the right to correct, rectify, restrict or erase information that is regarded as wrong, or to object to processing.
- Take appropriate technical and organizational security measures to safeguard personal information
- Ensure that personal information is not transferred outside of the EEC without suitable safeguards
- Ensure that any breaches of data protection are dealt with in accordance with legal requirements including reporting to the ICO where this appropriate

Derbyshire County Council's Measures to achieve its Commitment to Data Protection

Derbyshire County Council will adhere to the principles of the Data Protection Act 2018 by ensuring the following.

- There are officers with specific responsibility for data protection in the Council. The Data Protection Officer is the Deputy Director of Legal Services. The Caldicott Guardian is the Director of Adult Care. The SIRO is the Director of Finance and ICT.
- Everyone at the Council managing and handling personal information is trained appropriately (compulsory Information Governance course)
- Everyone at the Council managing and handling personal information is supervised appropriately
- Anyone at the Council who does not normally handle personal information knows what to do if the occasion arises
- Subject access requests and queries about personal information are dealt with promptly and courteously and where there is to be a legitimate delay this is explained
- Policy and guidelines on handling personal information are published, and are clear and up to date

- Regular reviews are undertaken of the way personal information is managed and handled in the Council
- Regular assessments are made of the Council's compliance with the GDPR and the Data Protection Act 2018
- Incidents involving breaches of this policy are recorded and analysed, and disciplinary action taken as appropriate
- This policy integrates with other corporate policies associated with data protection and the identification of risk
- This policy is reviewed regularly and updated when necessary

Record of Processing

Under Article 30 of the GDPR the Council is required to have a record of processing in place.
The Information Commissioner's advice is that the following information is required to be included:

- *Your organisation's name and contact details.*
- *If applicable, the name and contact details of your data protection officer – a person designated to assist with GDPR compliance under Article 37.*
- *If applicable, the name and contact details of any joint controllers – any other organisations that decide jointly with you why and how personal data is processed.*
- *If applicable, the name and contact details of your representative – another organisation that represents you if you are based outside the EU, but you monitor or offer services to people in the EU.*
- *The purposes of the processing – why you use personal data, e.g. customer management, marketing, recruitment.*
- *The categories of individuals – the different types of people whose personal data is processed, e.g. employees, customers, members.*
- *The categories of personal data you process – the different types of information you process about people, e.g. contact details, financial information, health data.*
- *The categories of recipients of personal data – anyone you share personal data with, e.g. suppliers, credit reference agencies, government departments.*
- *If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.*
- *If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is*

based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR.

- *If possible, the retention schedules for the different categories of personal data – how long you will keep the data for. This may be set by internal policies or based on industry guidelines, for instance.*

- *If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training*

  The Council has 5 Registers in place as a consequence of its GDPR preparation activities. These are as follows (with links to Website or EDRM);

  (1) Information Audit Register
  (2) Contracts (Personal Data) Register
  (3) Data Sharing Agreements Register
  (4) Privacy Impact Assessments Register
  (5) Corporate and Departmental Risk Registers

  Each Department of the council has also adopted a series of retention schedules. These can be found at; www.derbyshire.gov.uk/retentionschedules

  The Council considers that taken collectively these Registers and schedules provide the information that is required to be documented under Article 30. For the avoidance of any doubt however the Council wishes to respond to the bulleted paragraphs as follows;

  - The Data Controller is Derbyshire County Council. County Hall Matlock Derbyshire
  - The Council's Data Protection Officer is Simon Hobbs, Deputy Director of Legal Services
  - Any joint control of data is shown in the Register of Data Sharing Agreements
  - The categories of personal data and individuals are contained within the Registers
  - The Council does not presently operate outside of the EEC
  - The purposes of processing are contained within the Information Risk Register. The Council carries out only very limited marketing activity.
  - The categories of recipients of personal data are indicated with in the Information Risk Register, the Data Sharing Agreement Register and the Contracts Register
  - Personal data is sometimes transferred outside of the EEC by the Council's Data Processors under contracts, but where this happens, the Council requires the processor to ensure that the transfer will take place either on the basis of an adequacy decision under GDPR Article 45 or that appropriate sharing safeguards have been put in place pursuant to GDPR Article 46.

- The Council has retention schedules in place which can be found at; www.derbyshire.gov.uk/retentionschedules
- The Council has extensive provisions in place for data security https://www.derbyshire.gov.uk/working-for-us/data/if-something-goes-wrong/report-a-security-incident.aspx and for compulsory training of all staff which arrangements are overseen by its Information Governance Group chaired by the SIRO, Peter Handford.

Appropriate Policy Document

Under Schedule 1 Part 4 to the 2018 Act there is a requirement for the Council to have a policy document in place for the purposes of relying on a condition set out in Part 1, 2 or 3 of Schedule 1 of the Act.

Under Part 4 paragraph 39 the document must

(a) Explain the controller's procedures for complying with Article 5 in connection with the processing of personal data and
(b) Explain the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition giving an indication of how long such personal data is likely to be retained.
(c) The contents of this Data Protection Policy constitute the Controller's procedures for complying with Article 5
(d) The contents of the retention schedules contained at www.derbyshire.gov.uk/retentionschedules constitute the Controller's policies as regards the retention and erasure of personal data.

The Council as a processor

Where the Council provides services to a third party (which includes for these purposes county schools as well as aided schools and academies) which involve personal data it is likely that the Council would be considered to be a processor within the meaning of Section 59 of the 2018 Act.

Accordingly the Council confirms that it will comply with Sections 59 (2) to (4) of the Act.
In relation to Section 59 (5) of the Act it is not legally possible for the Council to contract with County schools. Accordingly the Council will agree in writing via an SLA, where appropriate, the matters referred to in section 59 subsections (5), (6) and (7) of the 2018 Act .

Suggested KPI's for Data Protection Policy

- Number and percentages of subject access and freedom of information requests completed within statutory timescales
- Number and nature of information security incidents
- Number and percentage of the workforce who have completed mandatory Information Governance training

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