ISMS DOC REF	ISMS DOC 05
Review date	January 2018
Version No.	v5.0

Information Governance Framework

Schedule 03A

Data Protection and Confidentiality Policy

This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website http://www.northlincs.gov.uk/your-council/information-and-performance/information-governance/

Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.

Background Information	
Document Purpose and Subject	To provide a corporate policy for Data Protection and Confidentiality.
Author	Information Governance & ICT Security Function.
Document Owner	Information Governance & ICT Security Function.
Last Review	Last Review – January 2017.
Reference and Version	ISMS DOC #
Change History	V5.0 - The policy has been refreshed and amended so that it is more concise and easier to apply. The Access to Information parts of the policy have been moved to the Access to Information Policy so that this policy concentrates on the other requirements of Data Protection and Confidentiality. The Data Protection Act is replaced by the General Data Protection Regulation on 25 May 2018 and the Policy also starts to introduce this new Regulation.
Issue Date	11 April 2018
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	15 March 2018

Contents

1. Introduction

The Data Protection Act 1998 (DPA) implements the European Data Protection Directive in the UK and it came into force on 1st March 2000. This is being replaced on the 25 May 2018 by a European Regulation called the General Data Protection Regulation (GDPR). The Information Commissioner's Office (ICO) is the regulator for the Data Protection legislation in the UK.

For both pieces of legislation the requirements are divided into rights given to individuals and organisational obligations. The main changes brought about by the GDPR include organisations such as the council having to demonstrate compliance, the definition personal data being expanded and additional rights being given to individuals.

The DPA and GDPR apply to personal information processed by organisations such as the council. To operate efficiently we have to collect and use (process) personal information about the individuals. These include members of the public, current, past and prospective employees, clients and customers, and suppliers. We take compliance with the Data Protection legislation very seriously.

The council is the Data Controllers for the personal information it holds or is held on its behalf when it determines the purposes and means of processing. As a Data Controller the council could face enforcement action from the Information Commissioner's Office (ICO) for non-compliance with Data Protection legislation. This could include a monetary penalty up to £500,000 under the Data Protection Act and up to £18 million under the General Data Protection Regulation. Liability could extend to individual employees in certain circumstances, such as if personal information were to be unlawfully obtained or disclosed and this could result in disciplinary action or a personal fine. Sometimes there will also be another joint Data Controller who could share the liability.

The council also appoints Data Processors who are responsible for processing personal data on its behalf and may also be a Data Processor at times for another organisation. Under the General Data Protection Regulation the council is obliged to ensure there is a contract in place and that the processor complies with the GDPR. Under the GDPR Data Processors may also be subject to fines or other sanctions if they don't comply.

The aim of this policy is to set out how we will comply with the DPA and the GDPR when processing personal information.

This policy is part of a suite of Information Governance and ICT policies and procedures.

2. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the council.

Schools, who are Data Controllers in their own right, may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

3. When do the Data Protection Act Apply?

In the Data Protection Act the word 'data' means information that:

- Is processed automatically;
- Is recorded with the intention that it will be processed automatically;
- Is recorded as part of a relevant filing system or with the intention of being part of such as system;
- Does not fall within the above three categories but which forms part of an accessible record, such as health records, educational records (local education authority and special schools only), local authority housing records and local authority social service records;
- Is recorded and held by a public authority which does not fall within the above four categories.

A 'relevant filing system' is one where information is organised either by reference to individuals or by criteria relating to individuals so that a specific detail about a person may be easily selected from the system.

Personal Data is that which could identify someone either directly or indirectly.

Sensitive Personal data under the DPA is defined as data about: racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

4. When does the GDPR Apply?

Under GDPR Personal Data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online

identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include:

- Race;
- Ethnic origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life; or
- Sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

In order to lawfully process special category data, we must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

5. Principles of the Data Protection Act

We have a duty under the DPA, unless an exemption applies, to comply with eight legally enforceable principles, as summarised below.

Personal information should be:

1. Fairly and lawfully processed;
2. Obtained for specified purposes and not used for other incompatible purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;

5. Not kept for longer than necessary;
6. Processed in line with the rights of individuals;
7. Kept secure;
8. Not transferred to countries outside of the European Economic Area unless adequate protection is assured.

6. Principles of the GDPR

From 25 May 2018 we have a duty under the GDPR, unless an exemption applies, to comply with six legally enforceable principles as summarised below.

Article 5 of the GDPR requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. 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;
6. Processed in a manner that ensures appropriate security of the personal data.

We are also responsible for demonstrating compliance with the above principles.

7. Compliance with the Data Protection Act & the GDPR

We will, through appropriate management ensure that anyone authorised to access personal information takes appropriate care by:

1. Observing the conditions regarding the fair and lawful collection and use of personal information;
2. Specifying the legal basis, purpose and condition for processing for the personal information being processed and by not using this information for another incompatible purpose and from 25 May 2018 under GDPR documenting and publishing this and other information about the processing including the legal basis relied upon to process the personal data;
3. Collecting and processing only the appropriate amount of information needed to fulfil operational needs or to comply with any legal requirements;

4. Ensuring the quality of personal information created, used and held;
5. Keeping personal information secure;
6. Applying strict checks to determine the length of time personal information should be held and ensuring it is not kept for longer than is necessary or disposed of too soon;
7. Ensuring that individuals are aware of their rights under the DPA and from 25 May 2018 their rights under the GDPR and are able to exercise them;
8. Only applying exemptions as permitted by the DPA and from 25 May 2018 those permitted by the GDPR.
9. Ensuring that any third parties contracted by the council to process personal data adhere to appropriate controls and that appropriate checks are carried out to ensure compliance;
10. Only transferring personal information outside of the European Economic Area (EEA) when permitted by the DPA and from 25 May 2018 the GDPR, to ensure that assurance is in place that the personal data will be adequately protected;
11. Appointing a Data Protection Officer who is adequately trained, has the necessary resources and who is involved in Data Protection decisions at the highest level in the organisation.
12. Investigating and responding to complaints in relation to the DPA and from 25 May 2018 the GDPR, as set out in the Information Complaints Policy.
13. Investigating and responding to security incidents and possible data breaches as set out in the Security Incident and Data Breach Policy.

8. Data Protection Officer

The GDPR requires certain organisations, such as the council to appoint a Data Protection Officer from 25 May 2018. The role was optional under the DPA but was recognised by the council.

Under GDPR Data Protection Officers must fulfil certain duties including being:

- Trained to enable then to provide the necessary advice to the councils;
- Involved in decisions about how personal data is processed and have access to senior management when necessary to communicate compliance recommendations.
- Visible by having their contact details published by the council to enable individuals to make contact with Data Protection concerns.

9. Rights of Individuals under the Data Protection Act

The DPA provides individuals with certain rights, as below:

1. **Request a copy of their personal information** - these requests are known as 'Subject Access Requests' or 'SARs' and further information can be found in the Schedule 05A Access to Information Policy.
2. **Request that inaccurate information be rectified, erased, destroyed or blocked** – information will be amended or deleted or a note will be attached explaining why this is not possible.
3. **Prevent processing for direct marketing** – if the councils carry out direct marketing these activities will stop in response to a request from an individual.
4. **Prevent automated decision taking** – if the councils are making a significant decision about an individual just using automated means individuals have the right to request human input.
5. **Seek compensation** - an individual, who suffers material damage or distress as a result of the councils not complying with the DPA principals, is entitled to seek compensation if it can be demonstrated that reasonable care to comply was not taken.

Requests should be made in writing to the contact details shown in Appendix B and we will respond in writing to explain any action taken or why the request cannot be met. We will also provide advice with each response about how to make a complaint.

10. Rights of Individuals under the GDPR

The GDPR provides the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

6. Notification to the Information Commissioner

We are required under the DPA to notify the Information Commissioner's Office (ICO) annually of what personal information is being processed. Each notification is published on the ICO website www.ico.org.uk and can be viewed by searching the Register of Data Controllers.

The North Lincolnshire Council registration number is Z563337X.

Notification arrangements under GDPR had not been confirmed when this policy was approved but will be added to future revisions as they become known.

7. Records of Processing

From 25 May 2018 the GDPR requires us to demonstrate compliance with the legislation. To comply we must publish Records of Processing for all instances where personal data is processed by the council to explain how and why the data is being processed. The Record of Processing template is shown as Appendix A.

8. Privacy Notices

Under DPA there is the requirement for the council to be transparent about personal data processed by putting Privacy Notices in place to explain about this processing.

There is a general Privacy Notice on the council's website. Additional more specific Privacy Notices are created and these are clearly stated where necessary on written literature, council web pages and verbally, if individuals are being spoken to face to face or by telephone.

Under the GDPR the information that must be included within Privacy Notices is set out in the legislation.

9. Privacy by Design

The councils have adopted Privacy by Design and Default principles that mean privacy requirements and Data protection compliance are taken into account as part of day to day work and during projects when processes are being designed and systems implemented. The Privacy Impact Assessment process explained in the next section is used to assess privacy risk and to aid compliance with Data Protection legislation.

10. Privacy Impact Assessments & Data Protection Impact Assessments

Privacy Impact Assessments (PIAs) are carried out as part of the Integrated Impact Assessment process on major council decisions and projects if personal information is involved and there are risks to the privacy of individuals and to non-compliance with the DPA.

The following questions are considered when deciding whether or not to carry out a PIA:

1. Will new personal information be collected?
2. Will personal information be disclosed to organisations or people who have not previously had access to the information?
3. Will personal information be used for a purpose it is not currently used for, or in a way it is not currently used?
4. Is new technology to be used that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition technology?
5. Will decisions be made or action taken about individuals in ways that can have a significant impact on them?
6. Is personal information involved that is particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be extremely private.
7. Will individuals be contacted in ways that they may find intrusive?

The PIA Template in Appendix C will be used to carry out the assessment and record the results.

Under GDPR these assessments will be known as Data Protection Impact Assessments. This policy will be updated when full details are known.

11. Data Protection Audits

Under GDPR there is a requirement for the council to carry out audits to understand the obligations that must be complied with and to identify any gaps.

Appendix A – Record of Processing Template

1. GDPR Record of Personal Data Processing			
Processing Ref		Date of Review	
Nature of Activity			
Function			
Description of functions carried out			

2. Data Controller / Data Processor Details	
Data Controller	
Details of any Joint Data Controllers	
Details of any contracts in place	
Details of any Data Processors	
Details of any Data Processor Agreements	
Information Asset Owner	

3. Processing Purpose Details	
Description of the purpose (reason) for processing personal data	
Basis for the processing of the personal data	
Link to privacy notice and/or Link to awareness raising materials	
Details of any Privacy Impact Assessments carried out	
Does the processing involve automated decision making, including profiling	
Is personal data used for direct marketing purposes	

4. Details of Personal Data Processing	
Categories of data subjects	
Categories of personal data being processed	
Source of the personal data	
How is the personal data collected?	
When is the personal data collected?	
Estimate of the number of records	

held	
Retention period(s) in place for the personal data	
5. Recipients of Personal Data (in the UK)	
Categories of the recipients of the personal data	
Safeguards in place for the transfer of the personal data	
Details of any Information Sharing Agreements in place	
6. Recipients of Personal Data (outside of the UK)	
Categories of the recipients of the personal data	
Details of any transfers of personal data outside of the UK - to a third country or to an international organisation	
Safeguards in place for the transfer of the personal data	
Details of any Information Sharing Agreements in place	
7. Processing Measures in Place	
Technical and organisational measures in place for data security and protection	
Format information is held in	
Systems data is held on	
If the data includes health data has processing been approved?	
8. Any Additional Information	
9. Non Published Information	
Completed by	
Team manager	
Details of any data downloads	
Ability to block access to individual records and when this is actioned	
Ability to destroy data in systems	
10. Non Published Information	
Contact Details	
Contact Details	

Appendix B – Contact Information

North Lincolnshire Council Contacts

Telephone (Informal complaints only)	01724 297000
Email	customerservice@northlincs.gov.uk
Post	Customer Feedback, Civic Centre, Ashby Road, Scunthorpe DN16 1AB
In Person	By contacting one of our advisors at a Local Link Office – listed below

North Lincolnshire Council Local Links

Ashby & District Local Link	Ashby High Street, Scunthorpe, DN16 2RY
Barton Local Link	Providence House, Holydyke, Barton, DN18 5PR
Brigg & District Local Link	The Angel, Market Place, Brigg, DN20 8LD
Crowle & North Axholme Local Link	52 – 54 High Street, Crowle, DN17 4DR
Epworth & South Axholme Local Link	Chapel Street, Epworth, DN9 1HQ
Scunthorpe & District Local Link	Church Square House, 30 – 40 High Street, Scunthorpe, DN15 6NL
Crosby Local Link	Citizens Advice Bureau, 12 Oswald Road, Scunthorpe, DN15 7PT
Winterton & District Local Link	West Street, Winterton, DN15 9QJ

How to contact the Information Commissioner

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Telephone: 0303 123 1113 or 01652 545700;
Email: notification@ico.gsi.gov.uk; Web: www.ico.gov.uk

Appendix C – Privacy Impact Assessment Template

Step One - Identify the need for a PIA
(Summarise why a PIA is required)

Step Two - Describe the Information Flows
(Describe how personal information will be collected, used and deleted and how many individuals are likely to be affected)

Step Three - Consultation Requirements
(Explain who should be consulted internally and externally to ensure that all privacy risks have been explored and how this will take place)

Step Four – Identify the Privacy Related Risks
(Identify the key privacy risks and any associated compliance or corporate risks – larger projects might record this information on a formal risk register).

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Organisation / Corporate Risk

Step Five – Identify Privacy Solutions
(Describe the actions you could take to reduce risks)

Risk	Solution(s)	**Result –** is the risk eliminated, reduced or accepted?	**Evaluation –** is the final impact on individuals after implementing each solution a justified, compliant & proportionate response to the aims of the project?

Step Six – Sign off and Record the PIA Outcomes
(Who has approved the privacy risks involved in the project and what solutions need to be implemented?)

Step Seven – Integrate the PIA Outcomes back into the Project Plan
(Who is responsible for integrating the PIA outcomes back into the project plan & updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?)

Action to be taken	Date for Completion of Actions	Responsibility for Action

Contact Point for Future Privacy Concerns

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and
b) for sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?	
How will you tell individuals about the use of their personal data?	
Do you need to amend your privacy notices?	
Have you established which conditions for processing apply?	
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	
Have you identified the social need and aims of the project?	
Are your actions a proportionate response to the social need?	

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?	
Have you identified potential new purposes as the scope of the project expands?	

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?	
Which personal data could you not use, without compromising the needs of the project?	

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?	
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?	
Are you procuring software that will allow you to delete information in line with your retention periods?	

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?	
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?	
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?	
If you will be making transfers, how will you ensure that the data is adequately protected?	