# Legal Responsibilities Policy

May 2022

| | |
|---|---|
| **Version Number** | 1.1 |
| **Approved by** | Corporate Policy and Resources Committee |
| **Date approved** | 27/10/2016 |
| **Review Date** | May 2022 |
| **Authorised by** | Director of Resources |
| **Contact Officer** | Data Protection Officer |

# Table of Contents

# 1 Overview

This Policy lists and describes the legislation and regulations that govern information management and highlights the risks both to the organisation and to individuals for failing to comply.

# 2 Purpose

At West Lindsey District Council ("the Council") we create, collect, hold, and use vast amounts and types of information to carry out our functions, much of which is governed by legislation. For instance, we process personal data about people and organisations with whom we deal with, information protected by copyright, and intellectual property which we must keep confidential.

In addition, we are occasionally required by law to collect and use certain types of personal information to comply with the requirements of Government departments.

However, we also make much of our information publically available to demonstrate open and transparent government and Information Rights legislation such as the Freedom of Information Act 2000 sets out how we must publish or respond to legitimate requests for our information

This Policy details our responsibilities under the wide and varied legislation that governs our information and information systems.

# 3 Scope

Any information must be dealt with properly irrespective of how it is collected, recorded and used, whether on paper, in a computer, or recorded on other media. For instance, there are safeguards set out in the UK General Data Protection Act and the Data Protection Act 2018 to make sure that personal information is collected and processed correctly.

This Policy relates to all information held or processed by the Council. It applies to all full time and part time employees of the Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers and students or trainees on placement with the Council, who have access to information held or processed by the Council.

# 4 Roles and Responsibilities

For most information-related legislation the following Council officers are accountable and responsible for compliance. Where specific responsibilities exist for legislation, these are included within the description of the particular legislation below.

- **Chief Executive**. The Chief Executive has overall responsibility for strategic and operational management, including making sure that Council policies comply with all legal, statutory and good practice guidance requirements.

- **Senior Information Risk Owner (SIRO).** The SIRO has overall responsibility for ensuring that information risks are properly recorded and managed.

- The Assistant Financial Director is the Council's Section 151 Officer with responsibility for exercising the proper administration of the Council's financial affairs under section 151 of the Local Government Act 1972 and section 114 of the Local Government Finance Act 1988.

- **Data Protection Officer (DPO).** The DPO is accountable to the Board for the management of personal information within the Council and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

    - development and implementation of the Personal Information Management System (PIMS) as required by the Data Protection Policy; and
    - security and risk management in relation to compliance with the policy.

- **Information Asset Owners (IAO).** IAOs will be senior members of staff who are the nominated owners for one or more identified information assets of the Council. It is a core information governance objective that all information assets of the Council are identified and that their business importance is established.

- **Corporate Information Governance Group (CIGG).** The CIGG is chaired by the SIRO and comprises the information specialists from across all service areas who can share knowledge and experience where necessary. The group has a pivotal and central role in ensuring that Information Governance is effectively communicated and managed and across the organisation.

# 5 Policy

This section lists the legislation applicable to information and information systems and details specific responsibilities for complying with it.

## 5.1 Civil Contingencies Act 2004

Category 1 organisations (the emergency services, local authorities, NHS bodies) are at the core of the response to most emergencies and are subject to the full set of civil protection duties.

The act requires that, as Category 1 Responders, Local Authorities put in place Business Continuity Management arrangements.

### 5.1.1 What will the Council do?

In order to meet its obligations under the Act, the Council will:

- Assess the risk of emergencies occurring and use this to inform contingency planning;

- Put in place emergency plans;
- Put in place business continuity management arrangements;
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;
- Share information with other local responders to enhance co-ordination;
- Co-operate with other local responders to enhance co-ordination and efficiency; and
- Provide advice and assistance to businesses and voluntary organisations about business continuity management (applicable to local authorities only).

#### 5.1.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.2 Companies Act 2006

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

#### 5.2.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

#### 5.2.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.3 Common Law of Confidentiality

Common Law of Confidentiality is not in any written Act of Parliament. It is "common" law which means that it has been established over a period of time through the courts.

The law recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that:

- it is not "trivial" in its nature;

- it is not in the public domain or easily available from another source;
- it has a degree of sensitivity; and
- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a solicitor/client, health practitioner/patient, etc.

However, as with the Human Rights Act 1998, confidentiality is a qualified right[1]. The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.

### 5.3.1 What will the Council do?

In order to meet its obligations under the Common Law of Confidentiality, the Council will make sure that:

- Confidentiality is included as an essential element of employee terms and conditions;
- The need to keep information confidential where appropriate is included in all security awareness training.
- Confidentiality clauses are included in all Council contracts where information may be accessed or shared.

### 5.3.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will recognise and understand the importance of not disclosing confidential information to anyone who does not have a "need to know" and will comply with Council's policies and procedures relating to this legislation.

### 5.3.3 Roles and Responsibilities

Everyone who comes into contact with information has a responsibility to keep it private where necessary and in some cases may be held personally accountable for any breach of confidentiality.

[1] Qualified Rights are rights which can be restricted not only in times of war or emergency but also in order to protect the rights of another or the wider public interest. In general, qualified rights are structured so that the first part of the Article sets out the right, while the second part establishes the grounds on which a public authority can legitimately interfere with that right in order to protect the wider public interest

### 5.4 Computer Misuse Act 1990

The computer misuse act makes it illegal to gain unauthorised access to a computer. The act is made up of three separate offences:

Unauthorised access to computer material; the act of accessing materials without authorisation is an offence even if no damage is done, files deleted or changed.

Unauthorised access with intent to commit or facilitate commission of further offences.

Unauthorised modification of computer material; including the amendment, damage of data, including the introduction of computer viruses.

#### 5.4.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements and the penalties for offenses under the Act are included in awareness training provided to staff, Members and partners.

#### 5.4.2 What will the Council's employees do?

As well as not committing any of the 3 basic offences, Council employees and other parties listed at para 3 must not:

1. Display any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate hacking)

2. Display any information that may lead to any unauthorised modification of computer materials (such modifications would include activities such as the circulation of "infected" software or the unauthorised addition of a password)

3. Display any material, which may incite or encourage others to carry out unauthorised access to or modification of computer materials.

#### 5.4.3 What are the consequences of non-compliance?

The penalties for committing criminal offences in each of the 3 categories are as follows:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer which carries a penalty of up to six months imprisonment or up to a £5,000 fine.

2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking which carries a penalty of up to five years of imprisonment and an unlimited fine.

3. Unauthorised modification of computer material, which includes:

i) intentional and unauthorised destruction of software or data;

ii) the circulation of “infected” materials on-line; and

iii) An unauthorised addition of a password to a data file.

This offence carries a penalty of up to five years of imprisonment and an unlimited fine.

## 5.5 Copyright, Designs and Patents Act 1988

The law gives the creators of literary, dramatic, musical, artistic works, sound recordings, broadcasts, films and typographical arrangement of published editions, rights to control the ways in which their material may be used.

The rights cover; broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public.

In many cases, the creator will also have the right to be identified as the author and to object to distortions of his work. International conventions give protection in most countries, subject to national laws.

### 5.5.1 Types of work protected

1. **Literary**. Song lyrics, manuscripts, manuals, computer programs, commercial documents, leaflets, newsletters & articles etc.

2. **Dramatic**. Plays, dance, etc.

3. **Musical**. Recordings and score.

4. **Artistic**. Photography, painting, sculptures, architecture, technical drawings/diagrams, maps, logos.

5. **Typographical arrangement of published editions**. Magazines, periodicals, etc

6. **Sound recording**. May be recordings of other copyright works, e.g. musical and literary.

7. **Film**. Video footage, films, broadcasts and cable programmes.

The Copyright (Computer Programs) Regulations 1992 extended the rules covering literary works to include computer programs.

Only software that is developed by the Council, or either licensed or provided by a developer to the Council should be used.

The copyright of all software developed within the Council by staff or contractors should be held by the Council.

The right of the Council to make copies, for its own use, of any software provided must be retained by the Council.

Under no circumstances should software be copied from one machine to another without the appropriate licence agreement. Only staff authorised by ICT management may install, or move software.

### 5.5.2 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

### 5.5.3 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation. Specifically, employees and other authorised users of the Council's ICT equipment will not install or use software, or use images, media or other copyrighted material that has not been approved and/or licensed for Council use.

### 5.5.4 What are the consequences of non-compliance?

Copyright infringement that may be criminal offences under the Copyright, Designs and Patents Act 1988 are the:

- Making copies for the purpose of selling or hiring them to others;
- Importing infringing copies (except for personal use);
- Offering for sale or hire, publicly displaying or otherwise distributing infringing copies in the course of a business;
- Distributing a large enough number of copies to have a noticeable effect on the business of the copyright owner;
- Making or possessing equipment for the purposes of making infringing copies in the course of a business;
- Publicly performing a work in knowledge that the performance is unauthorised;
- Communicating copies or infringing the right to "make available" copies to the public (either in the course of a business, or to an extent prejudicial to the copyright owner); and
- Manufacturing commercially, importing for non-personal use, possessing in the course of a business, or distributing to an extent that has a noticeable effect on the business of the copyright holder, a device

primarily designed for circumventing a technological copyright protection measure.

The penalties for these copyright infringement offences may include:

- Before a magistrates' Court, the penalties for distributing unauthorised files are a maximum fine of £5,000 and/or six months imprisonment;

- On indictment (in the Crown Court) some offences may attract an unlimited fine and up to 10 years imprisonment.

### 5.6 UK General Data Protection Regulation

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

**The Six Guiding Principles of the GDPR**

1. Lawfulness, transparency and fairness
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Confidentiality and integrity

The Council must be able to demonstrate compliance with these principles. This is **accountability** and can be considered as a “seventh” principle.

### 5.7 Data Protection Act 2018

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.

It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner’s functions and powers.

In order to meet its obligations under the Data Protection Act, the Council will make sure that:

- There is an individual with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are legally responsible for following good data protection practice.
- Everyone managing and handling personal information is properly trained to do so and adequate advice and guidance is available.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Methods of handling personal information are regularly assessed and evaluated.
- All actual or potential breaches of the Data Protection Act are investigated, mitigated, and reported as appropriate.

### 5.7.1 What will the Council's employees do?

Employees and agents of the Council are personally responsible for complying with the Data Protection Act. In particular they will make sure that:

- They attend or complete data protection training provided by or on behalf of the Council.
- When collecting or processing personal information in the course of their duties they follow any policies, guidance, and procedures provided by the Council for that purpose.
- They report any breaches of the Act using the Council's Data Protection Breach Policy.
- Queries about handling personal information are promptly and courteously dealt with.

### 5.7.2 What are the consequences of non-compliance?

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice of up to £17.5mil on a data controller.

### 5.7.3 Roles and Responsibilities

- The **Chief Executive** has overall responsibility for strategic and operational management, including ensuring that Council policies comply with all legal, statutory and good practice guidance requirements.

- The **Council's Senior Information Risk Owner** has overall responsibility for ensuring that information risks are properly recorded and managed.

- The **Council's Data Protection Officer** will provide guidance and advice to employees to facilitate the correct handling of personal information and to enable the Council to meet its legal obligations under the Data Protection Act.The DPO is responsible for notifying the Information Commissioner's Office of the Council's purposes for processing personal information.

- **Directors** are responsible for ensuring that the Council's Data Protection procedures are communicated and implemented within their directorates.

- **Information Asset Owners** are responsible for ensuring that all their staff are appropriately trained with regards to Data Protection and for ensuring that any Data Protection related issues in their own area are handled in compliance with this policy and relevant procedures. IAOs are also responsible for ensuring that all personal data is disposed of securely and in line with the Retention Guidelines for Local Authorities.

- All **Council employees** must attend relevant Data Protection training.

- All **Council employees** are responsible for understanding, and adhering to this Policy and the Council's Policy and procedures relating to Data Protection.

- All **Council employees** should seek Data Protection advice from the Council's Data Protection Officer when necessary.

### 5.7.4 Sharing Personal Information with other Organisations

Personal information must not be disclosed to any other person or organisation via any insecure method.

Where such information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Agreement.

The Council's Data Protection Officer is responsible for the Information Sharing Agreements.

## 5.8 Environmental Information Regulations 2004

The Environmental Information Regulations provide members of the public with the right to access environmental information held by public authorities.

Environmental information covers:

- The state of the elements of the environment, such as air, water, soil, land, fauna (including human beings);
- Emissions and discharges, noise, energy, radiation, waste and other such substances;

- Measures and activities such as policies, plans and agreements affecting or likely to affect the state of the elements of the environment;

- Reports, cost-benefit and economic analyses;

- The state of human health and safety and contamination of the food chain; and

- Cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

The Council is required to respond to a request for environmental information within 20 working days although further reasonable details can be requested to identify and find the information in line with the legislation.

#### 5.8.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

#### 5.8.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.9 Freedom of Information Act 2000

Gives a general right of access to all types of recorded information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Subject to the exemptions, any person who makes a request to a public authority for that information must be informed whether the public authority holds that information. If it does, that information must be supplied, subject to certain conditions.

Every public authority is required to adopt and maintain a publication scheme setting out how it intends to publish the different classes of information it holds, and whether there is a charge for the information.

Two codes of practice (s. 45 and s. 46) issued under the Act provide guidance to public authorities about responding to requests for information, and records management. The Act is enforced by the Information Commissioner.

### 5.9.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

### 5.9.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.9.3 What are the consequences of breaching the Act?

The Council may be breaching the Freedom of Information Act if it does any of the following:

- Fail to respond adequately to a request for information;
- Fail to adopt the model publication scheme, or do not publish the correct information; or
- Deliberately destroy, hide or alter requested information to prevent it being released.

This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

Other breaches of the Act are unlawful but not criminal. The Information Commissioner's Office (ICO) cannot fine the Council if it fails to comply with the Act, nor can it require us to pay compensation to anyone for breaches of the Act. However, we should correct any mistakes as soon as we are aware of them.

## 5.10 Human Rights Act 1998

An individual's privacy and protection of property rights must be respected. This includes ensuring the security of personal data. Infringements could lead to breaches of these rights.

An employee's privacy is, however, subject to the provisions of the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

### 5.10.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

### 5.10.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

## 5.11 Privacy & Electronic Communications (EC Directive) Regulations

The Privacy and Electronic Communications Regulations (PECR) originally came into force in 2003 and were amended in 2004, 2011, and again in 2015. The regulations sit alongside the Data Protection Act and give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- Marketing calls, emails, texts and faxes;
- Cookies (and similar technologies);
- Keeping communications services secure; and
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

### 5.11.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

### 5.11.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.11.3 What are the consequences of not complying with the Regulations?

The regulations carry a number of sanctions for non-compliance. These are enforced by the ICO and include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice imposing a fine of up to £500,000.

## 5.12 Re-use of Public Sector Information Regulations 2015

The Regulations are concerned with the re-use by businesses and citizens of information held by public sector bodies. "Re-use" essentially means the use of existing information in new products and services. Its aim is to support technology driven growth and civil society applications, for example, in the use of mapping information in satellite navigation products.

The Regulations affect how information can be re-used once it has been legitimately accessed, by placing obligations on the public sector to the benefit of re-users.

The Regulations do not create rights of access to information. They do not override or modify data protection rules. Re-use of public sector information in the UK must therefore comply with the Data Protection Act and any related regulations

#### 5.12.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

#### 5.12.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

### 5.13 Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA is the law governing the use of covert techniques by public authorities. It requires that when public authorities, such as the police or government departments, need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.

RIPA's guidelines and codes apply to actions such as:

- Intercepting communications, such as the content of telephone calls, emails or letters;
- Acquiring communications data: the 'who, when and where' of communications, such as a telephone billing or subscriber details;
- Conducting covert surveillance, either in private premises or vehicles (intrusive surveillance) or in public places (directed surveillance);
- The use of covert human intelligence sources, such as informants or undercover officers; and
- Access to electronic data protected by encryption or passwords.

RIPA applies to a wide-range of investigations in which private information might be obtained. Cases in which it applies include:

- Terrorism
- Crime
- Public safety
- Emergency services

#### 5.13.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

#### 5.13.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

# 6 Policy Compliance

## 6.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements required by the Data Protection Act 1998 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004 these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Corporate Policy and Resources Committee.

## 6.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer being the City Solicitor and the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

## 6.3 Policy Review

This Policy will be reviewed every two years by the Corporate Information Governance Group and approved by the Corporate Policy and Resources Committee. Authority to approve interim updates may be delegated to the Director of Resources in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee as required.

## 7 Related Standards, Policies, and Processes

- Information Governance Policy
- Data Protection Policy
- Freedom of Information and Environmental Information Regulations Policy.
- Information Sharing Policy
- Data Quality Policy
- Data Protection Breach Policy
- Records Management Policy
- Information Security Policy
- Retention and Disposal Policy