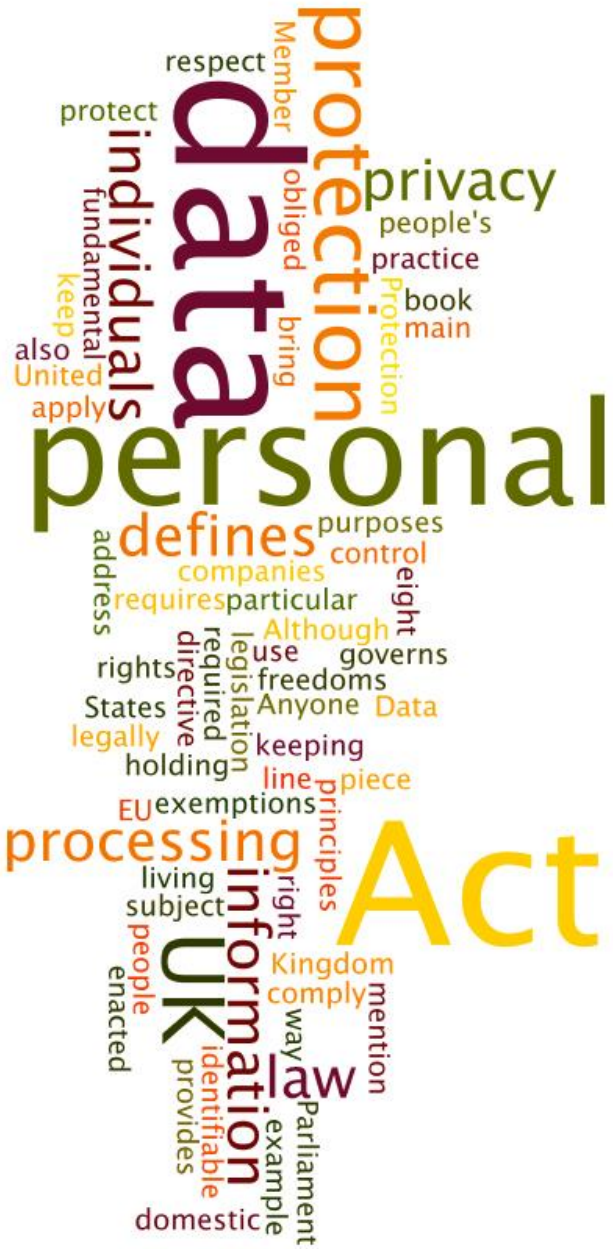

For queries regarding this policy, please contact:

Democratic Services Manager and Deputy Monitoring Officer.

WARWICK DISTRICT COUNCIL
www.warwickdc.gov.uk

Data Protection and Privacy Policy

Revision History

Document	Data Protection and Privacy Policy
Author	Graham Leach
Date Completed	9 February 2018
Review Date	*December 2021*

Version	Revision Date	Revised By	Revisions Made
1.0	February 2018	Graham Leach	Original Document
2.0	*November 2019*	*Shafim Kauser*	*Update with reference to Data Protection Act 2018*

Approvals
This document requires the following approvals:

Name	Date
Information Governance Manager	*07/11/2019*~~15/3/2018~~
ICT Manager	*07/11/2019*~~15/3/2018~~
SIRO	~~15/3/2018~~
Executive	~~5/4/2018~~

Distribution
This document has been distributed to:

Title
All Staff
All Members
WDC Website

Table of Contents

1 Management Summary

1.1. This is a key policy in a set that is underpinned by a number of other related policies, codes of practice and guidelines that form the WDC's Information Governance Framework. The Framework covers the wider requirements for compliance with information law and best practice.

1.2. Data Protection Legislation requires Warwick District Council to handle personal information relating to living identifiable individuals in a fair, safe, responsible and secure manner. There are other rules relating to information privacy, such as, the Privacy and Electronic Communications Regulation and the common law of confidentiality. In additional a range of information is defined as exempt from disclosure under the Freedom of Information Act and should also therefore be treated as private and confidential.

1.3. This policy sets out the Council's requirements regarding the appropriate and responsible use of personal and private information.

1.4. Data Protection Legislation *includes* ~~and~~ the General Data Protection Regulation *(GDPR), Data Protection Act 2018 (DPA), Privacy and Electronic Communications Regulation (PECR) Human Rights Act 1998 (HRA) that* attempts to strike a balance between the privacy rights of individuals and the legitimate interests of other parties who need to *collect and process* ~~access~~ that personal information for specified purposes.

1.5. The Council deals with individuals' personal information every day, in all sorts of formats, much of which is very private. ~~Much~~*Some* of this personal information is shared with other organisations (~~mainly~~*e.g. Data processors*, contractors and government bodies), mostly in the interests of the individuals concerned *to deliver the services required* but it may also be *shared* ~~used~~*where it is lawful to do so*. ~~for purposes deemed to be in the public interest~~.

1.6. The Council expects everyone who works on its behalf to recognise their responsibility for treating personal and private information with the care and respect it deserves. The same applies to those bodies with which the Council shares personal information.

1.7. The effect of a data protection breach can be very distressing and damaging to the individual concerned, and can also be damaging for the party responsible for the breach. The law does not create unreasonable barriers to the use of personal or private information, but it does subject individuals and organisations to significant sanctions for unfair, unlawful, disproportionate, or reckless use of private data.

2 Policy Statement

2.1 Warwick District Council regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining the confidence of those with whom we deal. We will always do our utmost to ensure that our organisation treats all information lawfully and correctly.

2.2 To this end we fully endorse the requirements of the General Data Protection Regulation (GDPR) and Data Protection Legislation

3 Purpose

3.1 To ensure that all managers and staff apply appropriate measures to comply with the requirements of the ~~GDPR and~~ Data Protection Legislation and so meet the Council's statutory requirements and avoid any incidents involving personal information that might cause harm or distress to individuals or cause the Council to incur statutory penalties.

4 Scope

This policy applies to:

- all employees
- all workers who are not employees (e.g. individuals supplied through an agency or other company or partner or subsidiary organisations, contractors, individuals seconded to the Council or otherwise engaged on Council business)
- all volunteers and any individuals on work experience at the Council
- all Councillors.

Any reference in this document to "employee" is deemed to be a reference to any of the above.

Note that the access to information and rights aspects of Data Protection Legislation are covered by the Access and Rights Policy.

5 Policy Requirements

There are a number of requirements set out in this Policy under the following headings:-

- The Council's Data Protection and Privacy Commitment
- The Data Protection Principles
- 'Special Data'
- Data Protection Breaches

The Council's has other policies, sub-policies and guidance on the use of personal information, which also form part of the Council's Information Governance Framework.

5.1 Data Protection and Privacy Commitment

The Council has made a Data Protection and Privacy Commitment which explains the approach taken by the Council to comply with the Data Protection Legislation, the Human Rights Act 1998, the duty of confidence, other legislation and best practice relating to the use of personal information. Everyone to whom this policy applies is required to meet the Data Protection *and Privacy* Commitment.

The Data Protection and Privacy Commitment is as follows:

The Council will seek to meet its obligations in law and in spirit by ensuring that we:-

- **Value the personal information entrusted to us** and make sure we respect that trust. There should be no surprises for the data subject in the way that we process, use or share their personal information. The data subject will be already well informed before we use their data.

- **Go further than just the letter of the law** when it comes to handling personal information, and adopt good practice standards, that ensure transparency and accountability.

- **Address privacy risks first** when we are planning to use or hold personal information in new ways, such as when introducing new systems. We will assess the risks and impacts on data subjects in a Privacy Impact Assessment document when required by data protection law.

- **Inform individuals when information will be shared** and why, and ensure that the organisations that we share information with fully comply with the information law.

- **Give access to data subject's information** when they request it, as well as processing updates and corrections in a timely manner. Please also refer to the Information Access and Rights Policy.

- **Keep personal information to the minimum necessary** and delete it when we no longer need it. The Council's record retention policy and schedule will be publically available and the information retention period for personal data will be stated when the information is collected.

- **Have effective safeguards in place to make sure personal information is kept securely** and does not fall into the wrong hands. The Council has an Information Security and Code of Conduct Policy and range of sub-policies including a *data~~n information~~* handling policy that deals with protective marking.

- **Provide awareness training *and regular refresher training* to all staff who handle personal information** and treat it as a disciplinary matter if they misuse or don't look after the information properly;

- **Put appropriate financial and human resources into looking after personal information** to make sure we can live up to our promises;

- **Regularly check that we are living up to this commitment** and report on how we are doing.

5.2 The Data Protection Principles

All employees must comply with the six *data protection* ~~GDPR~~ principles and the Council's policies and guidelines that underpin those principles, which state that an individual's personal information 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, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.3 Special *Category* Data *& Criminal Offence Data*

Data Protection Legislation makes it clear that there are some categories of personal information that require extra caution when handling:-

Special category data

- racial information
- ethnic information,
- health information,
- religious beliefs,
- political views
- sexual life,
- sexual orientation
- trade union membership,
- biometric data
- genetic data)

Criminal offence data

This relates to processing of criminal convictions and offences or related security measures and includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed.

Some special category data and criminal offence data may only be processed where the Council has an appropriate policy document in place. In cases where we process special category data in reliance of a condition set out in Schedule 1 of the Data Protection Act 2018, the Council has an appropriate policy document in place and the processing will be in compliance with the requirements of the General Data Protection Article 5 principles..

All those handling personal information must be aware of the extra sensitivity of these categories of personal information and be aware that any data protection breaches involving these will have correspondingly more serious consequences for the data subject and the Council.

5.4 Register of Processing Activity

The General Data Protection Regulation (GDPR) *(Article 30)* requires the Council to *maintain*~~keep~~ a record of *processing activities under its responsibility. This is a measure designed to demonstrate compliance with the accountability principle. To meet this responsibility, the Council maintains a Register of Processing Activity (ROPA) that includes* all personal datasets that it holds with essential details about collection (legal basis), use, security, sharing, and retention. This register must be kept fully maintained by the services teams collecting and using the personal data.

5.5 Data Protection Breaches

Any incident that could or does lead to loss, disclosure or temporary exposure of personal information must be reported as prescribed by the WDC Information Security Incident Management Policy and Procedure. The Council has procedures for investigating data protection and privacy breaches and all those affected will be expected to co-operate with any such investigation.

Certain types of personal data breach must be reported to the information Commissioner's Office. In such a case, the report will be made where possible ~~Serious data protection breaches will be reported to the Information Commissioner~~ by the Council's Data Protection Officer.

Disregard for the Council's data protection and related policies by employees may be regarded as misconduct to which the council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal. In the case of contractors, representatives, workers and volunteers, this may be grounds for termination of that relationship with the council.

Disregard for the Council's data protection and related policies by Councillors will be regarded as a breach of the Code of Conduct and will be considered in line with the adopted arrangements for the determination of complaints about Councillors.

6 Roles & Responsibilities

Every employee and other person to whom this policy applies is responsible for the appropriate use and protection of personal information which is in their possession or use. Everyone is also responsible for familiarising themselves with their obligations under this policy and related ones, for ensuring their own compliance and for seeking guidance where they need it.

6.1 The Executive

The Council's Executive are responsible for ensuring that sufficient resources are made available to support the Council and its employees in meeting the obligations under this policy.

6.2 Chief Executive and Deputy Chief Executives

The Chief Executive and Deputy Chief Executives are responsible for ensuring a co-ordinated response from the Council and its employees to this policy and for keeping under review the Council's approach to personal information, data protection and privacy.

6.3 Data Protection Officer

The Council has appointed an Information Governance Manager who will act as Data Protection Officer for the Council. They are responsible for reporting on Data Protection compliance, advising on Privacy Impact Assessments ~~for new systems~~ and liaison with the Information Commissioner over data breaches, data protection notifications and other issues as appropriate.

6.4 Heads of Service

Heads of Service are responsible for the information assets under their control including personal information.

- This includes identification, access, security, and privacy of personal information and updating their information asset details in the Register of Processing Activity (ROPA).
- They are responsible for making sure employees who access or handle personal information are suitably trained in data protection and privacy in order to understand their obligations under this policy.
- They will incorporate an assessment of data protection and privacy risk into their risk management arrangements as designated Information Asset Owners.
- Any new or amended systems for processing personal data must be screened for the possible need to produce a full Privacy Impact Assessment (PIA) as specified by the GDPR Privacy by Design requirement.

6.5 Managers

Managers are responsible for controls that ensure compliance with this policy. This will include:

- The induction of new staff,
- The implementation of compliant new procedures and systems
- Providing appropriate communications and awareness-raising of the policy requirements (both among employees and contractors with whom the deal)

7 Review & Revision

7.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2~~12~~months.
7.2 Policy review will be undertaken by the Council's Data Protection Officer.

8 References

8.1 The following Warwick District Council documents are relevant to this policy:

- Information Governance Framework
- Information Access and Rights Policy
- Information Security and Code of Conduct Policy
- Records Management Policy
- Information Security Incident Management Policy
- *Data Handling Policy*

9 Key Messages

9.1 The following are key messages from this Policy:

- All employees must comply with the Council's Data Protection and Privacy Commitment, the six Data Protection Principles and the all underpinning Council policies and guidelines.
- Special care must be taken when handling 'special' personal information.
- Any incident that could, or does lead to loss, disclosure or temporary exposure of personal information must be reported.