

Information Access and Rights Policy

Revision History

Document	Information Access and Rights
Author	Anna Moore
Date Completed	
Review Date	TBC once approved

Version	Revision Date	Revised By	Revisions Made
1.0	February 2018	Anna Moore	Original Document

Approvals

This document requires the following approvals:

Name	Title
Information Governance Manager	
ICT Manager	
SIRO	
Executive	

Distribution

This document has been distributed to:

Name	Title
All Staff	
All Members	
WDC Website	

Table of Contents

Information Access and Rights Policy	2
1 Management Summary	4
2 Policy Statement	4
3 Purpose	4
4 Scope	5
5 Policy Requirements	5
5.1 Privacy Notices	5
5.2 Consent	5
5.3 Access to Information – Guidance	6
5.4 Freedom of Information Requests	6
5.6 Subject Access Requests / Data Protection	6
5.7 Protective Marking	6
5.8 Fraud and Phishing	6
5.9 Personal Information Breaches	6
5.10 Other Rights - Rectification, Erasure, Restriction	7
6 Roles & Responsibilities	7
6.1 The Council's Executive	7
6.2 Chief Executive and Deputy Chief Executives	7
6.3 Data Protection Officer	7
6.4 Heads of Service	7
6.5 Managers	7
7 Review & Revision	7
8 References	7
9 Key Messages	8
APPENDIX	9

1 Management Summary

This document sets out the Council's policy in relation to both access to information and the exercise of information rights, including compliance with information law, primarily Freedom of Information and Data Protection legislation and the associated best practice.

This policy aligns with other policies in the Information Governance Framework, these are:-

- the Data Protection and Privacy Policy,
- the Information Security and Conduct Policy; and,
- the Records Management and Retention Policy.

There is also more detail guidance in sub-policies and procedures also falling within the scope of the Information Governance Framework.

This policy is to ensure that the Council gets the balance right between:-

- Being transparent and proactive by making information accessible whenever it can be and by disclosing and sharing information when necessary.
- Being helpful in ensuring people can exercise their information rights.
- Protecting information that needs to be retained, secure and confidential.

The issues covered are:-

- Privacy Notices
- Data Subject Consent
- Freedom of Information requests.
- Data Protection Subject Access) request handling.
- Protectively marked documents
- Self-service information
- Fraud and phishing.
- Other information rights

2 Policy Statement

Warwick District Council recognises that information rights are important in ensuring that the Council operates in a transparent and accountable way, but that they give the power to the individual to control the use of their personal information. This policy set out the Council's requirements in order to meet its legal obligations.

3 Purpose

The purpose of this policy is to ensure that:-

- Council's approach to access to information complies with legal, transparency and established best practice requirements.
- Services are aware of the broader information rights defined under data protection law and able to handle correctly and promptly with any request received.

More specifically to ensure that:-

1. When we collect or receive peoples' information they are provided with the details of how we use that information that we are required to give by law.
2. When we ask for a person's consent to collect and use their information, we do so according to data protection legal requirements.

3. Guidance is available to persons wanting to access either the Council's information or the information that we hold about them personally.
4. Requests for information are correctly identified. Not all will require a formal Freedom of Information response if they can be dealt with more quickly.
5. Requests for access to personal data are generally treated formally and include the necessary safeguards to prevent inappropriate disclosure.
6. Protectively marked are handled correctly under Freedom of Information. Data Protection and confidentiality law.
7. A self-service approach is actively encouraged where public information that is regularly requested can be made available on the WDC website using search facilities or by reference to the Publication Scheme.
8. Employees do not fall victim to phishing techniques or others involving fraud that are aimed at illegally obtaining access to confidential or personal information.
Where a requestor is invoking rights other than access to information, e.g. data rectification or erasure, services must ensure that these can be dealt with on a timely basis.

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.

5 Policy Requirements

5.1 Privacy Notices

When we collect or receive peoples' personal information they must be provided with the details of how we will use that information. The data protection legislation requires that the Council gives the detail shown in Appendix. The provision of this range of information is very important as the data subject needs it to exercise their rights. The Information Commission has set out very specific guidance on how this can be provided without information overload. This information must be provided for all existing and new uses of personal information.

5.2 Consent

Where consent is required to obtain personal information, because there is no other legal basis for collecting it, consent must be positively and unambiguously affirmed. No reliance can be placed on consent obtained by default, implied consent or inferred consent, and a record must be held of the consent. In addition it is no longer permissible to use consent as a legal basis for holding and using information where, for example, the information is necessary to perform a statutory function or any situation where the data subject has no effective choice. This approach must be taken to all existing and new uses of personal information involving consent.

5.3 Access to Information – Guidance

Guidance must be available to persons wanting to access either the Council's information or the personal information that we hold about them. This will be on the Council's website with links to and from the Council's top level Privacy Notice and to the Publication Scheme

5.4 Freedom of Information Requests

Requests for information under Freedom of Information Act (FOIA) or Environmental Information Regulations (EIR) must be correctly identified. The request does not have to name the Act or Regulation specifically and conversely the requestor may name the FOIA or EIR mistakenly when the request is for personal data. Deal with requests for publically available information as routine requests unless the information is more difficult to locate, complex in nature, or subject to possible restrictions. A self-service approach is encouraged for FOIA/EIR requests where public information that is regularly requested can be made available on the WDC website using search facilities or by reference to the WDC Publication Scheme.

5.6 Subject Access Requests / Data Protection

Requests for access to personal data will be treated formally and include the necessary safeguards to prevent inappropriate disclosure.

Everyone must however be aware that there are situations where personal information is disclosable:-

- For the prevention, detection and prosecution of crime
- Where there is a risk of significant harm to an individual.

There is more detailed information on dealing with these situations in the Confidentiality and Privacy Policy and the Guide to Information Requests (see 5.8 also Fraud and Phishing).

5.7 Protective Marking

Protectively marked records and information must be handled correctly under Freedom of Information, Data Protection and confidentiality laws. Be aware that the protective marking is a broad indication of the content and handling required. A more detailed examination of the document content may be required for FOI and DPA request purposes. There is more specific guidance on Protective Marking in the Information Handling Sub Policy

5.8 Fraud and Phishing

Not all requests for personal or confidential information will be genuine. Employees must be alert to the possibility that the person requesting the information may not be genuine. Fraudsters and phishers can be very credible. Anyone routinely applying for information in an official capacity must follow an established sharing protocol. There must be a sharing protocol in place for any routine sharing of personal or confidential information. For ad hoc confidential information sharing identity and authorisation checks must be carried out.

5.9 Personal Information Breaches

Information security issues are covered in the Information Security and Conduct Policy and breaches by the Incident Management Policy. Where an incident is likely to result in a high risk to the 'rights and freedoms' of a person the Data Controller shall notify the data subject without undue delay unless action has already been taken to address those potential concerns. This is partly to ensure that affected individuals can take timely action where this is needed.

5.10 Other Rights - Rectification, Erasure, Restriction

A requestor may invoke other rights e.g. data rectification or erasure etc. Services must ensure that these can be dealt with on a timely basis. The Appendix shows the other rights now available to data subjects. The Council is required to act on any such request without undue delay. Services must make sure that their information systems whether manual, network and email folder based, Electronic Records Management or Business Application enable the Council to fulfil those requests fully and reliably where they are found to be correctly invoked.

6 Roles & Responsibilities

6.1 The Council's 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 information access and data rights.

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 accountable, as Information Asset owners, for ensuring that all information risks relating to their information assets or service areas are properly assessed and action is taken where necessary to reduce the Council's information risk exposure.

6.5 Managers

Service Managers are responsible for ensuring that their service areas comply with this Policy and act to ensure that compliance is maintain, including for new or changed services or business processes.

7 Review & Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Council's Data Protection Officer.

8 References

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

- Warwick District Council – Information Governance Framework
- Warwick District Council – Data Protection and Privacy Policy

9 Key Messages

- Information rights are important in ensuring that the Council operates in a transparent and accountable way,
- These rights give some powers to the individual to control the use of their personal information.
- The Council must be able to respond to rights requests in an appropriate and timely way.

Privacy Notice Contents

Privacy Notices must to include the following information, but there is flexibility about how this is provided and the Information Commission advocate a tiered approach that provides information at the most appropriate time in the data collection process:

- The identity and the contact detail of the data controller.
- The contact details of the data protection officer.
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
- The right to withdraw consent where data is collected under this legal basis.
- The recipients of the personal data, or categories of recipients.
- Being informed about transfer outside the EEA and the personal data safeguards that would apply.
- The period for which the personal data will be stored, or the criteria used to determine that period.
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
- The right to lodge a complaint with the supervisory authority.
- The right to be informed of automated decision making including profiling as well as the significance and consequences for the data subject.
- Details of any further or secondary processing.