



Data Protection Policy

Version 3.0

| Document control | | |
|----------------------|--------------------------------|---|
| Document title | Data Protection Policy | |
| Purpose | | |
| Author | Information Governance Officer | |
| Date of publication | 15.04.18 | |
| Valid until | 15.04.19 | |
| Owner/responsibility | Brendan Whitworth | |
| Distribution | LanConsent/Other | |
| Version | Date | Comments |
| Version 1.0 | | |
| Version 2.0 | 10.10.11 | Approved by Head of Legal & Risk. Distributed 14.10.11 NetConsent. |
| Version 3.0 | May 2018 | Reviewed by A Roberts – policy now reflects GDPR requirements. |
| | | |

Data Protection Policy

1. Introduction

The EU General Data Protection Regulation (GDPR) is effective from 25th May 2018. GDPR signals the single biggest change in data protection in decades in that it replaces the Data Protection Act (DPA) 1998.

The main GDPR Principles

The data protection principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of *data subjects* (usually members of the public) for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a way 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.

Most people who work for Wigan Council use personal data. The Council's policy is to ensure that all personal information it obtains, uses or shares in its work is treated with care and respect, and used lawfully and fairly. The policy applies to data about employees as well as data about the public.

GDPR includes principles that explain how personal data should be used. The principles are flexible, and do not prevent effective working. Personal data can be obtained, used, shared and kept to provide services, look after people's interests, and support the Council's objectives. Data Protection legislation supports efficient working and reinforces the Council's objective to provide appropriate and personalised services. This policy sets out how GDPR and other data protection legislation applies to the Council, and sets out some specific measures to assist compliance.

2. Summary of Specific Measures

All departments will:

- ensure that all relevant staff attend mandatory training on data protection provided by the Data Protection Officer
- inform the Data Protection Officer of any new services, projects and processes involving the use of personal data, or of significant changes to existing ones. In certain cases it may be necessary to undertake a Data Protection Impact Assessment (DPIA) for 'high risk' data processing.
- report all losses, thefts or breaches of security involving personal data to the Data Protection Officer as quickly as possible
- Take steps (where practical) to anonymize personal data to mitigate against data security breaches
- notify the Data Protection Officer of all data or information sharing agreements or protocols
- participate in data protection audits
- Maintain an information asset register
- Appoint a senior officer to be accountable for managing information risk and for controlling the use, protection, sharing and timely disposal of personal information

3. Issues

3.1 Individual responsibility

The Council holds information about service users, local residents, elected members protect the personal data that they use, and be aware of their obligations. The use of personal data must be fair, legal and proportionate. Please note that the term "Personal Data" in this context includes any automated decision making or profiling systems. This includes:

- Web based forms
- E-mail addresses or cookies where a person's identity can be traced
- Biometric and facial recognition data

Staff cannot use personal data obtained at work for their own purposes. It is a criminal offence to knowingly or recklessly disclose personal data without the Council's permission. Anyone who uses, discusses or discloses personal data held by the Council without lawful authority may be committing an offence.

Staff who knowingly disclose or misuse Council data for their own purposes, or who

knowingly ignore the requirements of this policy may face disciplinary action, regardless of any possible criminal sanction. This could lead to dismissal in some cases.

Under GDPR fines can be issued where an organisation cannot demonstrate compliance with any of the principles. Fines could be up to €20million.

3.2 Awareness and training

We will promote the need to respect privacy and confidentiality so people remain confident about using Council services. People must be told how we will use their data, so that they are not reluctant to provide it to us. All staff must undergo mandatory Data Protection training applicable to their job role. The training module will be monitored on a regular basis by the Data Protection Officer to ensure compliance with relevant legislation and Council processes.

3.3 Obtaining information

People must be informed when we record information about them, unless there is a specific legal reason for not doing so. Any process involving the collection and use of personal data must conform to the GDPR principles. Managers must ensure that the use of personal data meets these conditions.

If third parties provide personal data to the Council, staff should inform the person concerned unless there is a valid legal or safety reason not to do so.

Consent (of the individual) is fundamental to compliance with GDPR and staff should ensure that consent is “Opt-in” with an option for consent to be withdrawn at any time. One caveat to this however is that where data processing is for a statutory purpose, consent will not be required.

The Data Protection Act 2018 lowers the age at which a child can provide consent (to data processing) from 16 to 13 years. It is essential that staff ensure that any necessary parental consent is obtained where appropriate.

3.4 New processes and services

Departments need to know the legal basis for using and sharing personal data when developing a new service or process, or ask the Data Protection Officer to identify it. The Data Protection Officer will carry out a Data Privacy Impact Assessment on new initiatives or existing services or projects, in any case where the impact is significant or intrusive.

If we need consent to use personal data, we will obtain it as soon as possible. If consent is not required, we will still tell people how their data will be used and the basis upon which it is being processed such as legal obligations.

In addition, Data Protection considerations will be built into the Wigan Council project management framework.

3.5 Application forms and tools to gather information

Any form or process (including an automated process) designed to gather information must include a simple explanation about why that personal data is needed, and what we will do with it. This 'fair processing notice' must also spell out whether data will be shared outside the Council. Existing forms without fair processing information will be amended when it is practical to do so.

3.6 Notification

The Council's notification to the Information Commissioner describes broadly how and why we use personal data; it is renewed annually every October. Departments should tell the Data Protection Officer immediately about new services or projects, or significant changes that might affect the notification. This in turn may necessitate a Data Privacy Impact Assessment to be undertaken.

The Data Protection Officer will process notifications on elected members' behalf.

3.7 Record Keeping

Departments must have in place adequate records management procedures, including measures to ensure that working records about people are fair, accurate, up-to-date and not excessive. Records about people must be secure, traceable and accounted for at all times. Each department must maintain and operate a retention and disposal schedule as part of the Council's [Records Management Policy](#). Records must be disposed of securely in accordance with the disposal schedule. Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

3.8 Extent of information

Personal data must be accurate, relevant, up-to-date, adequate and not excessive. It should be easy for staff and service users to update their data. Inaccuracies must be corrected as soon as they come to light. Staff should ensure that they keep enough information to provide an effective service, but avoid keeping data just in case it may become useful in the future. Service users should also be provided with details of:

- Who controls the data
- How it will be used and kept for
- How to correct any personal data that is incorrect
- The purpose for retaining the data

3.9 Need to know

Access to personal data must only be available to those who need it. If access to data is needed only some of the time, it should only be available some of the time. Data should be used when necessary, and not purely because it is convenient to

do so. This applies to all staff, including IT staff and non-technical staff with administrator or similar status. All access to systems containing personal data for maintenance or testing must be logged. Where a system has the facility to log the creation of users, this facility must be switched on.

3.10 Physical security

The Data Protection Officer must be notified of any loss, theft or accidental disclosure of personal data, or situations where this might have happened in accordance with [Wigan Council's Suspected Irregularity Reporting Protocol](#). All premises and electronic systems where personal data is held must include appropriate security. Access to areas where information is held should be controlled, paper files should be locked away when not in use and computer data must be protected by adequate security measures.

Electronic data must only ever be stored in official server rooms. If this is impractical, data must only be stored in locations agreed by the Data Protection Officer in consultation with the Computer Section.

It is Council policy to store data on a network server where it is regularly backed up.

Any use of Cloud technology for storing data should adhere to central government cloud security principles.

All valuable files and documents must be stored on the appropriate server on the Council's network and not on Desktop PCs or laptops.

Where information is gathered and recorded through mobile working then staff should download the data onto the appropriate network server as soon as possible.

Client data should not be on display except where necessary (i.e. for operational reasons or for safety reasons).

Encryption technologies will be employed to protect the security of data including emails.

Personal Data should never be stored on mobile devices, please see the [Use of Mobile Devices and Equipment Policy](#)

All data, physical or electronic, must be disposed of securely, in accordance with the Council's [retention and disposal schedule](#).

3.11 Validating requests for information

Departments must understand the legal framework that affects their work, so that they know when they have the power or the obligation to disclose information to other organisations, and to obtain it from them.

If an outside body requests personal data from the Council, staff must take

reasonable steps to check the identity and entitlement of the person requesting it. Requests for information should be made in writing to make clear what is required. If an outside body says they can demand personal data held by the Council, the legal basis of that right must be checked. Wigan Council's Data Protection Officer must be informed of all requests for information as a matter of urgency.

3.12 Security of transfer

Information should be shared by the most secure method available. When sending information outside the Council, staff must take steps to ensure that only appropriate people will see it and in accordance with the [Acceptable Use of IT Policy and Use of Mobile Devices and Equipment Policy](#).

3.13 Information-sharing agreements

An information-sharing agreement or protocol is not a legal requirement to share information – sharing can happen without one. An agreement does not create a legal gateway if one does not already exist.

All agreements or protocols between the Council and outside agencies must be registered with the Data Protection Officer. Departments must not sign an agreement without seeking advice. Agreements should be drawn up after consultation between organisations, not imposed by one on another.

Where information is shared between the Council and an outside agency, both parties must ensure that the data subject (Individual concerned) is informed about the details of why the information is being shared.

3.14 Contracts

If a contract or agreement involves the sharing of personal data, the contract should include measures to ensure that the data is used safely and appropriately. Information supplied to contractors can only be used for agreed purposes, and must not be used or disclosed for any other reason without further consultation with the Council, in such cases a Data Processor contract/agreement must be in place.

GDPR now changes the situation for Council contractors in that they will also be liable for any damage caused as a result of a culpable data breach. Standard contract clauses will detail the respective data responsibilities of both the Council and its contractors.

3.15 Access to Personal Data

Staff will assist individuals to get access to data that we hold about them. This might be by providing access to files, by advising them about the Council's procedures, or by referring them to the Data Protection officer. All 'subject access requests' (i.e. requests made by people for access to their own data) will (in most cases) be answered within 1 month.

Each Department will nominate someone as a first point of contact for subject access requests.

3.16 Complaints about personal data

If any person identifies errors or inaccuracies in the data we hold about them, or points out unfair uses of their data identified by requesters as a result of access to their files, these must be rectified immediately. We will immediately implement recommendations or instructions received as a result of an assessment or decision made by the Information Commissioner unless the Monitoring Officer believes the assessment to be incorrect.

3.17 Data Protection officer and Network

The Council will have a nominated member of staff with specific responsibility for data protection policy, advice, training and good practice. This is currently the Data Protection Officer in Legal Services.

The Council will maintain a network of staff trained in Data Protection issues who are available to provide advice to staff in all areas of the council and assist the Data Protection Officer. All Directorates will have a nominated Information Asset Owner (IAO) who will be at Assistant Director level. These IAO's will provide quality assurance and suggest areas to improve data security.

3.18 Induction

Information about confidentiality and data protection should be provided to all new members of staff. Basic guides to all data protection issues are available on the intranet.

3.19 Confidentiality

Information explicitly accepted in confidence or as part of a confidential relationship can only be disclosed to someone else in exceptional circumstances. Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them, unless the information is about serious wrong-doing or harm.

All staff have a duty to report any criminal activity or wrong-doing to the proper authorities if they become aware of it. The Council operates a [Whistleblowing Policy](#), which provides further advice on what to do in these situations.

3.20 Testing and Training

When developing or testing any new system or process, or working on an existing system, data about real people will not be used unless it is impossible to test the system without live data. If live data must be used for testing, please contact the Data Protection Officer.

Personal data must not be used in any training exercise – real examples must be fictionalised to the point where a person cannot be identified. Personal data can only be used for training purposes where managers or supervisors need to discuss with an officer the way they handled a specific case or situation.

3.21 Monitoring and Evaluation

The Data Protection Officer is responsible for ensuring that all departments understand the requirements of this policy and the relevant legislation. The Data Protection Officer will periodically audit departments using the Information Commissioner's audit guidance to ensure that we comply with the General Data Protection Regulation and supporting legislation.

3.22 Breach

Any breach of this data protection policy should be reported immediately to the Data Protection Officer. Thereafter a thorough investigation shall take place which is likely to include a referral to the Information Commissioner's Office.

3.23 Review of this policy

This policy will be reviewed by the Data Protection Officer on an annual basis to ensure that it takes account of new legislation and expected developments in the areas of personal privacy and public sector data sharing.

And employees, among others. Everyone who works for or represents the Council must