TRAFFORD
COUNCIL

Trafford Council

Data Protection

Policy, Statement and Guidance for Employees

Author	Paula Titterington
Date	January 2015
Status	Final
Version	3.0
Review Date	January 2017

Version Control

Document History

Issue	Date	Author	Change History
0.01	20/01/2014	Paula Titterington	First Draft
0.02	04/01/2016	Paul Fox	Second draft
3.0	July 2016	Mark Jones	Operational updates made

Document Reviewers

No.	Name	Role	Date	Issue
3.0	Mark Jones	Interim Head of Legal Services	July 2016	3.0

Document Approvals

No.	Name	Role	Date	Issue
3.0	ISGB	ISGB	23/08/16	3.0

Data Protection - Summary of Documents

The Data Protection Act 1998 (as amended) is to regulate the way that personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals to see the data stored about them and to require modification of the data if it is wrong and in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The Council has notified the Information Commissioner of its status as a Data Controller under the Data Protection Act 1998. The purpose of producing the following documents is to support the work of the Council in complying with, and to minimise the possibility of the Council breaching the legislation.

Data Protection Policy

This document sets out Trafford Council's policy regarding data protection. The policy applies to all staff and elected members, and to contractors, partner organisations and other third parties who may have access to the Council's information assets.

The Council has to ensure that the personal and sensitive information it holds about individuals is accurate, up to date, used only for the purpose intended and securely protected from inappropriate access. The Council also has to ensure that individuals can find out about their personal data, be given access to it and the right to challenge its accuracy.

The policy is based on the eight data protection principles, included at Appendix 1 of the policy. These principles are regarded as the minimum standards of practice for any organisation dealing with personal data.

Data Protection Statement

This important document informs the public about the information held and processed about them, and states what they should do if they have any questions concerning data held about themselves. The document summarises the Council's reasons for collection and use of personal data, and explains how the privacy of all personal information is maintained.

Guidance for Employees

The purpose of this document is to make staff aware of the responsibilities of the Council and of their own individual responsibility when collecting, holding, processing and sharing data, and dealing with subject access requests. It explains how the Act lays down rules regarding the way we handle data about people, the penalties should we get things wrong, and the rights people have in respect of accessing their personal information.

Trafford Council

Data Protection Policy

Commitment

Trafford Council is committed to ensuring that the personal and sensitive information it holds about individuals is accurate, up to date, used only for the purpose intended and securely protected from inappropriate access. The Council is further committed to ensuring that individuals can find out about their personal data, be given access to it and the right to challenge its accuracy. In terms of non-personal information, the Council is further committed to promoting public access to the information it holds.

Introduction

This document sets out Trafford Council's policy regarding data protection. The policy applies to all staff, councillors, contractors and partner organisations of the Council and other third parties who may have access to the Council's information assets.

The purpose of the data protection legislation is to regulate the way that personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals to see the data stored about them and to require modification of the data if it is wrong and in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The 1998 Act requires all processing of personal data to be notified to the Information Commissioner and all personal data to be kept and used in accordance with the provisions of the Act.

Data Protection Policy

The Data Protection Act 1998 requires the Council to comply with the Act when processing personal data.

1. The Council supports the objectives and principles of the Data Protection Act 1998 and recognises the need to maintain the confidentiality of all personal information held within the authority.

2. The Council requires all its staff and third parties who may have access to the Council's information assets to comply fully with this policy and the Data Protection Principles (attached at Appendix 1).

3. It may be a criminal offence to breach the provisions of the Data Protection Act 1998.

4. The Council will hold the minimum personal information necessary to enable it to perform its functions, and the information will be destroyed

once the need to hold it has passed. Every reasonable effort will be made to ensure that information is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay.

5. The Council recognises that personal information is confidential and that unauthorised disclosure is an offence under the Data Protection Act 1998. All information systems, manual or automated, containing personal data will therefore be designed to comply with the Data Protection Act 1998.

6. The Council will respect all individuals' rights under the Data Protection Act 1998. These include the right of any individual to ask whether the Council holds data on them, to be given a copy of such data and informed of the source of any data held.

   The Council will comply with such a request provided it is:
   - in writing
   - accompanied by sufficient information to assure the Council of the individual's identity
   - accompanied by sufficient information to enable the Council to locate the information requested
   - accompanied by the appropriate fee, currently £10, and
   - not subject to an exemption under the Act.

   The Information Governance Manager will be informed immediately of any such requests, which will be recorded centrally. He will ensure that agreed procedures and timescales are adhered to, to ensure that the most appropriate officers handle the request and monitor progress.

   If complying with a subject access request involves disclosure of information from which another individual can be identified, the Council will seek the consent of that individual, except where the Data Protection Act 1998 does not require this. If consent is not given the Head of Service of the service area involved, or a nominated representative, will make a decision as to whether to disclose, partly disclose or withhold the data. A written record of this decision will be passed to the Information Governance Manager who will hold it on file. If, in exceptional circumstances, consent of third parties cannot be sought, a decision will be made as if consent had been withheld.

   Individuals who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased and will receive a written response indicating whether or not the Council agrees and if so, the action to be taken. In the event the Council disagrees, the data subject may request their objection be recorded with the relevant record. In such circumstances, the relevant data will be marked "Under Dispute", with an appropriate dated file note of explanation.

7. Personal information will be disclosed only for legitimate purposes and in accordance with the Data Protection Act 1998 to:

- The data subject
- The courts under direction of a Court Order
- Any organisation having legal power to demand disclosure
- A third party where the appropriate consent has been obtained from the data subject
- For Special Purposes, at the discretion of the Data Controller
- Any other recipient providing the disclosure is in accordance with the provisions of the Data Protection Act 1998.

The Council is committed to working with outside organisations to improve services to local residents. In these circumstances information may be shared, but would only be released with appropriate safeguards or with consent to ensure that the rights of the individual concerned are properly protected.

8. It is the responsibility of Heads of Service to ensure compliance with this policy. Heads of Services may nominate a Liaison Officer to act on their behalf. An up to date list of Liaison Officers will be maintained by the Information Governance Manager

All computer systems and manual records within service areas which contain information about individuals must be identified, made secure and notified to the Information Governance Manager for notification purposes. All employees have a responsibility to co-operate with this task. If the Council's policy on data protection is not being complied with, the Chief Executive will take such steps as are necessary to secure compliance.

9. Where personal data is being collected from either a data subject or a third party, regardless of the method of collection, the data subject or third party will be given the information in section 10 below.

10. The information referred to in section 9 is:
    - All purposes for which the data will be kept or used
    - Any other information required to ensure data is processed fairly, that the data subject is fully aware of the intended use of the data and, where appropriate, that the data subject is informed of the identity of the Information Governance Manager at the Council.

11. Data will not be used for any purpose other than that the data subject has been made aware of unless the subject's consent is sought and given, except where this is permitted by the Data Protection Act 1998. A record will be kept by the officer authorised to use the data of any consent sought, given or refused.

12. In cases where the Council holds data as a consequence of providing services individuals, that data will not be disclosed without consent being obtained from that individual, except under the direction of a Court Order. Outside organisations using or sharing the Council's data

processing facilities will be responsible for notifying the Information Commissioner of their systems and for making any other arrangements needed to comply with the requirements of the Data Protection Act 1998.

13. In order to ensure the security and integrity of personal data held by the Council, no private use shall be made of any computer, tablet smartphone etc belonging to the Council, nor Council use of any computer, tablet, smartphone etc belonging to an employee, except in accordance with the Council's Acceptable Use Policy & Procedural Guidance.

14. All staff and other third parties who may have access to the Council's information will adhere to the authority's Data Protection Policy and comply with all security advice issued to prevent unauthorised access to personal information and to prevent it from being lost, stolen or rendered unusable.

15. Any losses of personal information or data breaches should be reported in accordance with the Security Incident Management Policy. Actual or potential breaches must be reported at the earliest possible stage as they need to be assessed by the appropriate officer, and notified to the Information Governance Manager, for reporting to the Information and Security Governance Board.

16. Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. A list of EEA countries can be found at Appendix 3.

    The Council will not publish personal data which is not already in the public domain on any internet site without the written consent of the data subject.

17. All staff and other third parties who may have access to the Council's information assets have regard to any such guidelines, codes of practice and procedures issued by the Council which relate to data protection. Disciplinary action may be taken against any employee who breaches any instruction contained in, or arising from this policy.

18. The full details of the Information Governance Manager for the Council are as follows:

    Information Governance Manager
    Legal Services
    Trafford Town Hall
    Talbot Road
    Stretford
    M32 0TH

Tel: 0161 912 1327

E-mail: data.protection@trafford.gov.uk

Appendix 1

DATA PROTECTION PRINCIPLES

The principles apply to all personal data processed by data controllers; controllers must comply with them, irrespective of whether they are required to notify and whether or not they are actually notified.

First Principle
“Personal data shall be processed fairly and lawfully.”

Second Principle
“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.”

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

Fourth Principle
“Personal data shall be accurate and, where necessary, kept up to date.”

Fifth Principle
“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.”

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

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

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

These principles, taken from the Data Protection Act, are regarded as the minimum standards of practice for any organisation with respect to personal data.

Appendix 2

Definitions - To aid the understanding of this document and provisions of the Data Protection Act the following definitions are provided:

Data is information that is:

- Being processed by means of equipment operating automatically in response to instructions given for that purpose, eg a payroll system
- Recorded with the intention that it should be processed by means of such equipment, eg on disk or CD ROM
- Recorded as part of a manual filing system or with the intention that it should form part of such a system, eg any departmental filing system with an index
- One of a number of records to which public access is allowed

Data Breach means an information security event or incident. These include an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a series of events that have a significant probability of compromising business operations and threatening information security.

Data Controller means the Council as the organisation who determines how data is processed.

Data Processor means any person, other than an employee of the Council, who processes data on behalf of the data controller, eg someone contracted to the Council to print documents containing personal data.

Data Subject is the individual about whom personal data is held.

Personal Data means data about a living individual who can be identified from that information (or from that and other information). This includes an expression of opinion about the individual.

Sensitive Personal Data means personal data consisting of information as to:

- Racial or ethnic origin of the data subject
- His or her political opinion
- His or her religious beliefs or other beliefs of a similar nature
- Whether he or she is a member of a trade union
- His or her physical or mental health or condition
- His or her sexual life
- The commission or alleged commission by him or her of an offence
- Any proceedings or sentence for any offence committed or alleged to have been committed by him or her.

Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information including organisation, adaptation or alteration, disclosure and destruction of the data.

Relevant Filing System means any manual filing system with an index

Special Purposes means any one or more of the following: journalistic, artistic or literary purposes.

Appendix 3

Countries currently within the European Economic Area

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom

Plus Iceland, Liechtenstein and Norway

Note that the Channel Islands and the Isle of Man are not part of the EEA

Trafford Council

Data Protection Statement

Trafford Council needs to collect and use information about people in order to operate effectively and efficiently and in the interests of everyone living in the area. This statement explains how we protect the privacy of all personal information which the Council holds.

1. The Council supports the objectives and principles of the Data Protection Act 1998 and recognises the need to maintain the confidentiality of all personal data held within the Council.

2. All Council employees, councillors and partner organisations are required to comply with the Data Protection Act 1998 and with the Council's own Data Protection Policy.

3. The Council will respect all rights established by the Data Protection Act 1998.

4. The Council will collect and hold the minimum personal information necessary to enable it to perform its functions and the information will be destroyed once the need to hold it has passed.

5. We will make every reasonable effort to ensure that information is accurate and up-to-date, and that where correction is needed, it is done without unnecessary delay.

6. When we collect personal information from or about you we will tell you what it is being used for and will not use it for anything else unless you give your permission, or unless we have a legal duty to do so. We will ensure that you are told who to contact if you have any questions about how your information is being used.

7. We will do all we can to ensure the security of your information to prevent unauthorised persons from accessing it and to prevent it from being lost.

8. If you have any questions about data protection in the Council please address them to:

   The Information Governance Manager
   Trafford Town Hall
   Talbot Road
   Stretford
   M32 0TH
   E-mail: data.protection@trafford.gov.uk

Trafford Council

Data Protection Act 1988 – Guidance for Employees

The purpose of this guide is to make staff aware of what they should be doing when requesting, holding, processing and sharing data, and dealing with subject access requests. It should be read in conjunction with the Council's Data Protection Policy document.

An introduction to the Data Protection Act 1998

All employees are required to comply with this policy. The Data Protection Act covers all uses of personal information, not just data on computer. You should ensure you are familiar with the policy and with your service area's own rules regarding the use of personal data.

This document will help to answer some of the most common questions about the Act.

The Data Protection Act

The Data Protection Act 1998 is a law designed to protect the privacy of individuals, in particular with regard to the processing of their personal information. It should be seen as a key part of human rights legislation. The Act came into force on March 1st 2000 as the result of a European directive. It has a far wider scope than previous legislation and incorporates changes arising from the way organisations now use data, changes in technology and experience of previous cases.

At the heart of the Act is a set of legally enforceable principles which must be complied with by "data controllers". A data controller is a person or (more commonly) an organisation having control over what data is collected and held and what it is used for. In our case "Trafford Council" is the data controller.

How does it work?

The Data Protection Act lays down rules regarding the way we handle data about people. It does not matter whether the information is on computer or in a paper filing system or even on a video or audio tape, a photograph or microfiche. If it is information about an identifiable, living individual the data protection rules must be followed.

What if I get it wrong?

There are penalties for the Council in the event that the Act is not complied with which could result in fines and compensation having to be paid. The Information Commissioner has the power to levy monetary penalties of up to

£500,000 in cases of breaches of the Data Protection Act. In some cases the individual who has broken the rules may be personally liable to prosecution. If you think anything in the way you work at the moment may need to be changed you should see your line manager as soon as possible. Your service area also has a Data Protection Liaison Officer who can help. Please ensure you know who your service area's liaison officer is.

What are the main points of the Act?

The Data Protection Act 1998 requires the Council to comply with eight Principles:

1. Data must be obtained and processed fairly and lawfully
2. It can only be used for the purposes specified in the organisation's notification entry or as otherwise allowed in law
3. The information on a person's record must be relevant in every case and should be no more than is necessary for the purpose for which it was obtained
4. The information should be accurate and should where necessary be kept up to date
5. Details must not be kept for longer than necessary for the stated purposes
6. Under the Act individuals have the right to see information held by the Council, and to have the information corrected or erased in certain circumstances.
7. There must be adequate security in place for manual and computerised information to prevent unlawful processing of the information and to protect against accidental loss or destruction of or damage to personal data
8. Personal data must not be transferred outside the European Economic Area without the informed consent of the individual, except where adequate protection exists in the country receiving it.

You should always ensure that anyone whose data you collect or use knows that you have it, why you have collected it, what it will be used for and how long it will be held for. This applies whether you have collected the information from the individual themselves, or it has been passed on from another source. You should always record where you obtained information from if it was not directly from the individual.

If you want to use information about individuals for a purpose that is different from that for which it was originally collected you will, in most cases, have to get consent from the individual first.

Guidance on the holding of information and the periods for which information should be retained is to be found in the Records Lifecycle Management Policy.

Guidance notes on specific issues under the Act may be issued from time to time. Employees should ensure that they are familiar with all guidance issued.

Are there any exceptions?

Exemptions in the Act allow for some information to be handled without all the provisions of the Act being applied. These include national security, crime and taxation (including Council Tax), disclosures required by law and others. You should not assume that an exemption applies to the work you are doing unless this has been confirmed for you. Your line manager or your service area's liaison officer can find out for you.

What rights do people have?

Everyone has the right to request a copy of the personal data held about them by any organisation and to request that it is changed if it is wrong, or deleted if it should not be held. The data controller can also be required to show the source of the information. When working with personal data you should remember this, and only record relevant items about people. Do not make "unofficial" comments about individuals in files, on sticky notes, by e-mail etc. Never write anything about another individual you would not be able and prepared to justify.

Guidance for employees concerning subject access requests – requests from individuals for information about themselves – appears on the intranet This guidance covers who can make a request, the receipt of and response to the request, and what to do in the case of disputed and inaccurate data.

What about security?

You should follow all security advice relevant to your service area, and which may be issued by the Information Governance Team. If you are not sure what is required of you, you should address any queries initially to your service area's liaison officer, or to the Information Governance Manager.

In particular, remember never to leave any personal data on view if it is not actually being worked on, always keep files secure and do not let anyone know your passwords for computer systems (unless exceptional circumstances warrant this).

Always wear your ID badge/swipe card and if you see anyone you do not know in the building without an ID badge ask if you can help them get to their destination.