TRAFFORD
COUNCIL

Trafford Council Data Protection Policy, Statement and Guidance for Employees

Author	Paul Fox
Date	April 2018
Version	5.0

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
4.0	April 2018	Paul Fox	GDPR and DPA updates made throughout
	20/04/2018	Wendy Trainor	Legal Review
5.0	27/04/2018	Stephen Girling	Formatting Edits

Document Reviewers

No.	Name	Role	Date	Issue
3.0	Mark Jones	Interim Head of Legal Services	July 2016	3.0
4.0	Wendy Trainor	Solicitor		4.0
5.0	Andrew Roberts	Senior Information Governance Officer	December 2021	5.0

Document Approvals

No.	Name	Role	Date	Issue
3.0	ISGB	ISGB	23/08/16	3.0
4.0				4.0
5.0	IAB	IAB	January 2022	5.0

Contents

Application

This Data Protection policy applies to the following:

- Council employees
- Elected Members
- Contractors
- Temporary staff
- Partner organisations
- Members of the public
- Volunteers
- Any other party utilising Council ICT resources

The provisions within this policy apply to all the groups listed above whether on Council premises or at any other location (3rd party organisation, working from home).

.

Summary of Documents

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 special category (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 six UK GDPR 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 and explain how personal information should be used.

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 DP legislation 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.

The protection of personal data belonging to Council employees is not within the scope of this policy. This is covered in the Council's Recruitment and Employment Privacy Notice.

Trafford Council Data Protection Policy

Commitment

Trafford Council is committed to ensuring that the personal and special category data (formally known as 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 are informed about their personal data, be given access to it and have 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, under the requirements of the Freedom of Information Act 2000.

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 DP legislation 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 it.

Data Protection Policy

The DP legislation requires the Council to comply with the Act when processing personal data.

1. The Council supports the objectives and principles of the UK GDPR 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 DP legislation

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 2018 and the UK General Data Protection Regulation (GDPR). All information systems, manual or automated, containing personal data will therefore be designed to comply with the DP legislation.

6. The Council will respect all individuals' rights under the DP legislation. 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:
   - made in writing or verbally
   - 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
   - not subject to an exemption under the DP legislation.

   The Information Governance Team will be informed immediately of any such requests using subjectaccessrequests@trafford.gov.uk so they are recorded centrally for monitoring purposes. It 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 DP legislation does not require this. If consent is not given the Information Governance team, will make a decision as to whether to disclose, partly disclose or withhold the data. A written record of this decision will be kept on file.

   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 DP legislation 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 DP legislation.

The Council is committed to working with outside organisations to improve services to local residents. In these circumstances personal information may be shared, but would only be released providing there was an appropriate legal basis.to do so or with the data subject's 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.

   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 this policy on data protection is not being complied with, the Data Protection Officer (DPO) 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 DPO at the Council.

Personal data may only be processed where there is a legal gateway to do so. Article 6 and Article 9 of UK GDPR provide more detail about what these provisions are but in most cases the Council will rely upon Legal Obligation (i.e. we are obliged to process data by law) **or** the processing is carried out in the public interest. Using consent as the legal basis is subject to specific requirements which are detailed in the guidance to employees in the body of this policy.

11. In cases where the Council holds data as a consequence of providing services to 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 (data processors) 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 DP legislation.

12. In order to ensure the security and integrity of personal data held by the Council, no private use shall be made of any computer, laptop, 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 and Procedural Guidance.

13. All staff and other third parties who may have access to the Council's information will adhere to this 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.

14. Any losses of personal information or data breaches should be reported in accordance with the Council's Security Incident Management Policy. Actual or potential breaches must be reported at the earliest possible stage to the Information Governance Team as they need to be assessed for reporting to the Information Assurance Board.

15. 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.
    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.

16. 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.

17. 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 2000
E-mail: data.protection@trafford.gov.uk

18. Governance

The Data Protection Officer (DPO)

Under the UK GDPR, it is mandatory for Local Authorities to designate a Data Protection Officer (DPO). This designation demonstrates a commitment to Data Protection and enhances the effectiveness of The Council's compliance efforts. The DPO is suitably qualified and has the necessary authority to provide guidance on all aspects of Data Protection. The DPO also has direct access to the Corporate Leadership Team (CLT).

The DPO's duties include:

- Ensuring the alignment of this Policy with Data Protection legislation
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs).
- Acting as a point of contact for and co-operating with the Information Commissioner's Office
- Determining the need for notification to the Information Commissioner's Office as a result of the Council's current or intended personal data processing activities.
- The operation of providing prompt and appropriate responses to Data Subject requests.
- Informing senior managers, officers and directors of any potential corporate, civil and criminal penalties which may be levied against the Council and/or its employees for a violation of applicable data protection laws.
- Monitoring compliance with Data Protection legislation
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this policy by any third party who;
    - Provides personal data to The Council
    - Receives personal data from The Council
    - Has access to personal data collected or processed by the Council

The DPO for Trafford Council is Dominique Sykes (data.protection@trafford.gov.uk)

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 DP legislation 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 DP legislation and with the Council's own Data Protection Policy.

3. The Council will respect all rights established by the DP legislation.

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 Data Protection Officer
Information Governance Team
Trafford Town Hall
Talbot Road
Stretford
M32 0TH
E-mail: data.protection@trafford.gov.uk

Trafford Council DP Legislation – 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.

All employees are required to comply with this policy. The DP legislation covers all uses of personal information, not just data on computers. 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 DP legislation.

Data Protection by Design

Data Protection Impact Assessments (DPIAs)

To ensure that all Data Protection requirements are identified and addressed, when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each requirement must go through an approval process before continuing.

The Council must ensure that a Data Protection Impact Assessment (DPIA) is conducted in co-operation with the DPO, for all new/revised systems or processes for which it has responsibility.

The subsequent findings of the DPIA must then be submitted to the Senior Information Risk Officer (SIRO) for review and approval.

The Data Protection Impact Assessment Policy and Procedural guide can be found on the Council's Information Governance intranet page.

Compliance Monitoring

Data Protection Compliance Audit

To confirm that an adequate level of compliance is being achieved by all users in relation to this Policy, the DPO will initiate routine Data Protection compliance audits to assess:

- Compliance with the policy in relation to the protection of personal data including assignment of responsibilities and training of employees.
- The effectiveness of data protection related operational practices.

- The level of understanding of data protection policies and privacy notices.
- The accuracy of personal data being stored.
- The adequacy of procedures for redressing poor compliance and personal data breaches.

Data Collection

Data sources

Personal data should only be collected directly from the Data Subject, unless one of the following applies:

- The nature of the business purpose necessitates collection of personal data from other bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject.
- If personal data is collected from someone other than the data subject, then the data subject should be informed unless one of the following applies;
    - The Data Subject has received the required information by other means: or,
    - The Information must remain confidential due to a professional secrecy obligation.

Where it is determined that notification to a data subject is required, this must be carried out no later than one month from the first collection or recording of the personal data.

Legal basis for Processing

In most cases the most applicable legal basis for processing personal data will be either:

- Compliance with a legal obligation, or:
- A task carried out in the public interest

In some circumstances processing may be carried out with the data subjects consent. Reliance on consent should not however, be the automatic default legal basis (For processing). Where consent is being relied upon it is important to note that there are specific conditions that need to be adhered to. These include:

- In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. This can be obtained by a written statement, including by electronic means, or an oral statement.

- The process for obtaining consent therefore, must include provision for:

    - Ensuring the request for consent is presented in a manner clearly distinguishable from other matters.
    - Ensuring the request for consent is made in an intelligible and easily accessible form, using plain language.
    - Ensuring consent is freely given (i.e. not based on a contract this is conditional to the processing of personal data).
    - Documenting the date, method, validity and content of the consent.
    - Providing a simple method for the data subject to be able to withdraw consent at any time.

- Once consent is withdrawn by the data subject, The Council must cease processing data for the specified purpose without undue delay.

Privacy Notices

The Council will provide data subjects with information as to the purpose of the processing of their personal data by way of a Privacy Notice.

Where any personal data is collected from the data subject, including where a data subject is asked to give consent to the processing of personal data, The Council will direct the data subject to a transparent Privacy Notices that details the following:

- Who you are
- What you are going to do with their information
- Who you will share their information with
- How long you expect to keep their information
- Contact details of the DPO

The Council will host a Primary Privacy Notice on the corporate website. This notice explains who we are, how we use personal information, advises about individuals privacy rights and how the law protects them.

All service areas that collect personal data must develop a service specific privacy notice relevant to their data processing activities. A Service Specific Privacy Notice guidance document is hosted on the Information Governance intranet page.

All service specific privacy notices must be approved by the DPO, prior to publication on The Council's corporate website.

Records of Processing Activity (ROPA) register

The Council will maintain a Records of Processing Activity register. Each record will contain (at least) the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed
- The legal basis for processing
- where applicable, transfers of personal data to a third country or an international organisation, including documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures

Keeping a record of the Council's processing activities is not a one-off exercise. The information documented must reflect the current situation as regards the processing of personal data. These records should be regarded as a living document to be updated as and when necessary.

Regular reviews of the personal data processing will be undertaken by the DPO to ensure all processing records remain accurate and up to date.

It is the responsibility of each Information Asset Owner (IAO) to ensure that this register is continually monitored for accuracy.

Data Processing

Processing Personal Data

The Council will process personal data in accordance with all applicable laws and contractual obligations. More specifically, The Council will not process personal data unless at least one of the following requirements is met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract, or prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect he vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

There are some circumstances where personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. Please seek advice from your DPO before any such processing commences.

Prior approval must be obtained from the DPO using the Data Protection Impact Assessment Policy and procedural guide when implementing new processes and the basis for the processing must be clearly recorded on The Council's Record of Processing Activity register.

Processing Special Categories of Data

The Council will only process special categories of data (also known as sensitive data) where the data subject explicitly consents to such processing, or where one of the following applies:

- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest.
- Further conditions include limitations based upon national law related to the processing of genetic data, biometric data or data concerning health and for reasons of public interest in the area of public health.

Processing of personal data relating to criminal convictions and offences will only be carried out under the control of the official authority pursuant to Article 10 of the UK GDPR and Schedule 2 Part 1 of the Data Protection Act 2018.

In each case, prior approval must be obtained from the DPO using the Data Protection Impact Assessment template contained within the Data Protection Impact Assessment Policy and procedural guide and the basis for the processing must be clearly recorded on The Council's Record of Processing Activity register.

Children's Data

Children under the age of 13 are unable to consent to the processing of personal data for information society services, which is any service normally provided at a distance, by electronic means and at the individual request of a recipient of services. Consent must therefore, be sought from the person who holds parental responsibility over the child.

Where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Should the Council, foresee a business need for obtaining parental consent for information society services offered directly to a child, guidance and approval must be obtained from the DPO before the processing of a child's personal data may commence.

Data Quality

The Council will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate. Measures to ensure data quality includes:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any data protection principles.
- Restriction rather than deletion relating to:
    - Law prohibiting erasure.
    - Erasure impairing legitimate interests of data subject.
    - The data subject disputing that the personal data is correct and it cannot be ascertained otherwise.

Profiling & Automated decision making

The Council will only engage in profiling and automated decision making where it is necessary to enter into/to perform, a contract with the data subject, or where it is authorised by the law. In such cases the data subject will be given the opportunity to:

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a human carry out a review of the automated decision
- Contest the automated decision
- Object to the automated decision-making being carried out.

Digital marketing

The Council will not send promotional or direct marketing material through digital channels such as mobile phones, email and internet without first obtaining explicit consent from the data subject.

Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to withdraw their consent to having their data processed for such purposes at any stage.

Once an objection to digital marketing is received, the Council must cease processing data for this purpose without undue delay.

Data Retention

Records Management

Departments must put 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 and be disposed of securely. Further details can be found in the Records Management Policy.

Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

Departments will regularly need to assure themselves that they are compliant with statute by reporting any discrepancies.

The length of time for which The Council needs to retain personal data is set out in the Corporate Retention Schedule, found on the Information Governance intranet page. All personal data should be deleted or destroyed as soon as possible, when it has been confirmed that there is no longer a need to retain it.

Archiving

All users are responsible for ensuring that personal data records that are required to be kept for archiving purposes are managed in line with the Records Management Policy and in accordance with the Corporate Retention Schedule.

Awareness and Training

All staff with access to personal data will participate in an on-going programme of mandatory data protection training. Staff are required to complete the training prior to accessing any personal information on Council systems. The annual completion of this training is mandatory. The training content is located on the Me Learning platform. Compliance checks will be made regularly to ensure all users are up to date.

Information Security

Physical Security and Breach Reporting

All premises and electronic systems where personal information is held must have adequate security. Access to areas where information is held must be controlled, paper files containing personal information must be locked away when not in use, and computer data must be protected adequately.

All users must adhere to the Council's Acceptable Use Policy which outlines the standards of conduct that are required of you when using all electronic communications and systems.

The Information Governance Team must be notified of any actual loss, theft or accidental disclosure of personal information. Further information can be found in the Security Incident Management Policy.

Any individual who suspects that a personal data breach has occurred due to theft or exposure of personal data must immediately notify the DPO.

The DPO will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the DPO will follow

the relevant authorised procedure based on the criticality and quantity of the personal data involved. For significant personal data breaches, The DPO will initiate an emergency response team to co-ordinate and manage the personal data breach response.

The Need to Know

Access to personal information must only be given to those who need it. Personal information should only be used when necessary and not purely because it is convenient to do so.

Each Information Asset Owner is responsible for restricting access to personal information and ensuring compliance with this policy.

All access to systems containing personal information for maintenance or testing must be logged. Where a system has the facility to log the creation of users, and the accesses those users have made, this facility must be switched on.

Complaints Handling

Data subjects with a complaint about the processing of their personal data are required to put forward the matter in writing to the DPO. An investigation of the complaint will be carried out to the extent that it is appropriate based on the merits of the specific case. The DPO will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the DPO, then the data subject may, at their option, seek redress through the Data Protection Authority (The Information Commissioner) within the applicable jurisdiction.

Data Subject Requests

The DPO is responsible for enabling and facilitating the exercise of data subject rights related to:

- Information access
- Objection to processing
- Objection to automated decision-making and profiling
- Restriction of processing
- Data portability
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, the DPO will consider each request in accordance with all applicable data protection laws and regulations.

No administration fee will be charged for complying with such a request unless the request is deemed to be unnecessary, excessive in nature, or a repeated request.

All subject access requests must be answered within 1 month following the date of receipt. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Controller however, must notify the data subject of any such extension within one month of receipt of the request together with the reasons for the delay.

All requests received for access to, or deletion/rectification of personal data must be directed to the DPO either by post or via data.protection@trafford.gov.uk
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 however, the use of a protocol will ensure best practice by all partners in any information sharing partnership.

All agreements or protocols between the Council and outside agencies must be registered with the Information Governance Team and agreed with the Senior Information Risk Officer (SIRO) and the DPO.

Departments must not sign any agreement without seeking advice from the DPO. Agreements should be drawn up after consultation between organisations, not imposed by one on another.

Information Governance must be consulted whenever a Department wishes to share information with either internal or external partners.

Security of Transfer

Security of Transfer to Third Party Data Controllers and Data Processors

The Council will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, The Council will first identify if the third party is considered a data controller or a data processor of the data being transferred.

Where the third party is deemed to be a data controller, The Council will, with assistance from the DPO, enter into an appropriate agreement with the controller to clarify each party's responsibilities in respect of the personal data transferred.

Where the third party is deemed to be a data processor, the Council will, with assistance from the DPO, enter into an adequate processing agreement with the processor to protect the personal data from further disclosure and to only allow processing in compliance with the Council's instructions.

The DPO will ensure that all transfers of data comply with appropriate technical and organisational measures to protect the personal data.

The Council will also ensure that all third parties are issued with the procedures for notification of personal data breaches.

Security of personal information disclosures

When sending personal information outside the Council, users must take steps to ensure that only appropriate people will see it.

If email is considered to be the best option, employees must use the correct email address and be aware that email inboxes may be monitored by managers or others who may not be entitled to access personal information.

Personal information must only be shared by secure transfer such as using an Egress email exchange.

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 employees have a duty to report any criminal activity or wrong doing to the proper authorities.

The Council operates a Whistleblowing Policy, which provides further advice on what to do in these situations. This Policy is on the Council's intranet.

Testing and Training

When developing or testing any new system or process, or working on an existing system for the purpose of testing or training, information about real people must not be used. This applies equally to users and 3rd parties when testing or upgrading systems. Personal information must not be used in any training exercise – real examples must be fictionalised to the point where a person cannot be identified.

Policy Compliance

The Council will ensure that users are aware of their responsibility for processing personal data along with the contents of this policy. In addition The Council will make sure that all third parties engaged to process personal data on their behalf are aware of and comply with the contents of this policy. Assurance of such compliance will be obtained from all third parties prior to granting them access to personal data controlled by The Council.

The Audit and Assurance section will periodically audit departments using the Information Commissioner's audit guidance to ensure that all parts of The Council comply with the current DP legislation.

If any user is found to have breached this policy, they will be subject to Trafford Council's disciplinary procedure. If a criminal offence is considered to have been committed further action will 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 DPO.

Review and Revision

This policy will be reviewed every year to ensure that it takes account of new legislation and expected developments in the areas of personal privacy and public sector information sharing.

Policy review will be undertaken by the DPO. The next review of this policy will take place in January 2024.

Appendix 1

THE UK GDPR 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 lawfully, fairly and in a transparent manner in relation to individuals."

Second Principle

"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes."

Third Principle

"Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."

Fourth Principle

"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Fifth Principle

"Personal data must be 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals."

Sixth Principle

"Personal data shall be 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."

These principles, taken from the UK GDPR, are regarded as the minimum standards of practice for any organisation with respect to personal data. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles. The principle of accountability also underpins the six principles above.

Appendix 2

Definitions

To aid the understanding of this document and provisions of the DP legislation 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, e.g. a payroll system
- Recorded with the intention that it should be processed by means of such equipment, e.g. 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, e.g. 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.

Special Category Data (sometimes called 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
- Genetic data
- Biometric data.

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.

Pseudonymisation is the processing of personal data in such a way that it can be no longer be attributed to a particular data subject without the use of additional information

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.