

The Data Protection Act 1998 Policy for Officers and Members

The Council prides itself on its respect for the privacy of the individual. Information held by the Council is a valuable asset and we owe a duty, both to the members of the public and to those who work for the Council, to protect their personal data from accidental or deliberate damage, disclosure or unauthorised modification or destruction.

This statement sets out the Council's policy on data protection and answers key questions relating to the proper management of personal data and to the rights and the responsibilities of those who work with personal data.

Data Protection Policy Statement

The Council complies with the Data Protection Act 1998. As part of this, all personal data we hold has been notified to the Information Commissioner. The Council's notification can be checked on line by logging on to www.dpr.gov.uk/search.html Please note that, for the purposes of this policy, 'data' includes all information including that held on manual files.

- a) This policy applies to all employees and elected Members as well as to contractors and external data processors instructed by the Council. Training will be provided to assist all the Council's staff and Members to comply with this policy.
- b) The Council will hold the minimum amount of personal data necessary to enable it to perform its functions. Every effort will be made to ensure that information is accurate and up to date and that inaccuracies are corrected without unnecessary delay.
- c) The Council will always obtain the express consent of a data subject to process personal data about that person if it is being held for any purpose that is not a statutory function of the Council.
- d) Any request by a data subject not to process personal data for a non-statutory function will be honoured.
- e) The purpose for which personal data is being held and why and to whom it can be disclosed will either be made known to the data subject in question at the time the personal data is being collected or made readily available to the data subject on request.
- f) Personal data will be accurate in respect of matters of fact. Opinions will be carefully and professionally expressed.
- g) The Council will respond to and assist every request for access to personal data from employees or members of the public.

- h) The Council will charge whatever the current maximum fee allowed is for access to personal data. Requests for access should be directed to the Data Protection Officer.
- i) Authorisation from a Council manager of at least third tier must be obtained before an employee is allowed to use a privately owned computer to process personal data belonging to the Council or to take personal data out of the workplace for processing on a computer owned by the Council or for any other purpose.
- j) Personal data will be kept in an appropriately controlled and secure environment both within Council premises and if any file containing personal data is removed from Council premises.
- k) Data sharing with external agencies will be the subject of a written agreement setting out the powers that permit the exercise, its scope and controls and will be agreed at the highest level.
- l) Any member of staff who knowingly or recklessly breaches the Council's Data Protection policy may be subject to disciplinary procedure.

Legal Definitions

Personal Data

Any personal information that is processed is readily accessible and relates either directly or indirectly to a living, identifiable person.

Data Subject

The individual to whom the information relates.

Data Controller

A named officer within the organisation who is ultimately responsible for the processing of data; for each system there is a data controller responsible for the data within that system. Within the Council there are many data controllers. The person with the ultimate responsibility within the Council for matters connected with the Data Protection Act is the Data Protection Officer who is currently the Head of Governance. The Head of Governance is also responsible for notifying the Information Commissioner of the personal data held and processed by the Council.

Processing

Obtaining, recording, holding or carrying out any set of operations on the information or data, including organising, adapting, altering, retrieving, consulting, using transmitting, disseminating, making available, aligning, combining, blocking, erasing or destroying.

Source

Where the data entered into a computer system or filing system originates from.

Disclosure Recipient

Organisations or individuals to whom the data can be given or disclosed.

Subject Access

Anyone who thinks that the Council is holding data about him or her is entitled to receive a copy of the information or to be told that no data is held about them. Applicants must identify themselves and specify which data they wish to see. Applications should in the first instance be made in writing to the Data Protection Officer. The Council is under a legal obligation to comply with a subject access request (SAR) submitted with the required fee (currently £10) within 40 days of its receipt.

Practical Guidance for Members and Officers

What does the Act mean for employees?

The Council is committed to compliance with this Act and assigned responsibility for this. Managers should ensure that their area of operation complies with the Act, that their use of personal data is registered and that staff are aware of the policy and procedures to follow. Each employee has an individual responsibility to make themselves aware of what the act involves and to comply with it.

What does the Act mean for Members?

Elected Members should make themselves aware of and comply with this policy when engaged on Council work. Members should ensure that their use of personal data in their constituency work is registered. There should be a clear separation between the data held for Council work and that held for constituency work.

How do I know if I can disclose personal data for a particular purpose?

Generally, data held by the Council is not to be disclosed outside the Council unless required by law. Disclosures within the Council are permitted if they are necessary for an officer to carry out their normal duty but the purposes must be compatible with the purpose for which it was originally gathered. There will be occasions when confidentiality will not even allow internal disclosure.

How do I deal with requests from external organisations to share data?

Requests from agencies such as the Police, a Health Authority, etc. should be cleared with the Data Protection Officer. If any agency proposes a long-term partnership in sharing data, a written agreement must be drawn up stating what powers it has to enter into such an agreement, who will manage the exercise and what controls will be in place. If a request is made regarding an individual, the agency making the request should specify why it requires it and the legal power it has for requesting such information. You must ensure that you have this in writing. Never disclose to a telephone enquirer or e-mail enquiry without checking first.

What about the public utilities?

Historically, disclosures were made to the public utilities but many of these are now private companies and no longer entitled to receive data from the Council or to disclose to it. If they are entitled to exchange data, they should be asked to make their case in writing and to quote the powers they have. Just because it may be beneficial to both parties does not mean that a disclosure is permitted in law. Information gathered for one purpose is generally limited to the use for that purpose only.

What about publicly available information?

Information in the public domain can be passed on.

What personal data does the Council hold?

The Council's notification is available for inspection on the Information Commissioner's website www.dpr.gov.uk/search.html. The Council's registration number for accessing its entry is Z6584640.

What about manual files?

Manual files are covered by the 1998 Act. Subject Access to manual files is permitted and any processing that involves manual files must be notified to the Information Commissioner.

Can we carry out 'Data Matching'?

'Data Matching' is the act of examining data held in two or more systems in order to check whether there is any recorded information common to both or all of those systems that indicates that the information relates to one and the same person.

The Council can carry out data matching if there is a clear justification for it such as the detection of fraud.

Does the Council disclose to the Police?

Local Councils may disclose to the Police for the purposes of the "prevention of crime or apprehension of offenders", anti-social behaviour and community safety as permitted under Section 115 of the Crime and Disorder Act 1998. There is no general disclosure to the Police.

Where can I get further advice?

Within the Council, you should consult with the Data Protection Officer (Head of Governance), Sue Carr (Professional Standards Officer) or Mandy Weir (Performance Officer). Always err on the side of caution: "When in doubt, check it out".

Checklist of Dos and Don'ts

- Do obtain consent for processing personal data that is volunteered in any situation where the Council is not performing one of its statutory functions
- Do inform anyone supplying personal data of the purpose for which that data will be held and what disclosures of it can be made
- Don't disclose any personal data held for a non-statutory function without first obtaining the consent of the person it relates to
- Do treat personal data with great care
- Do secure all personal data and dispose of confidential waste by shredding or using the blue bags provided
- Do ensure that no one else, especially members of the public, can read information, including e-mails, from your PC screen
- Don't allow papers containing personal data that you are reading in a public place, such as on the train, to be overlooked by anyone else
- Don't leave files unattended in your car when you take them out of the office
- Do use discretion when talking on a mobile phone or holding discussions with colleagues in places where your conversations involving personal data can be overheard by anyone else
- Don't use unauthorised software on your PC as this might result in corrupting data held on it
- Don't ever leave your PC logged on while you are away from it – for however short a time that might be - without using a password-protected screensaver

- Don't tell anyone your password
- Don't use personal data for any purpose other than that for which it was collected; if you want to collect additional data, your data protection notification will have to be amended (contact the Data Protection Officer immediately)
- Do check identities of enquirers before disclosing data
- Don't disclose to any person unless they have a need and a right to know; if in doubt, check it out with the Data Protection Officer
- Do inform the Data Protection Officer immediately about any communication you receive that you think is a subject access request to let a data subject know what personal data the Council holds about them
- Don't disclose to anyone not authorised in your notification to the Information Commissioner; if in doubt, contact the Data User
- Don't risk disciplinary action being taken against you by knowingly or recklessly failing to observe any of these dos and don'ts or any other part of this policy