

General Data Protection Regulation (GDPR) / Data Protection Act 2018 Policy



Signed: Claire Hamilton

Chief Executive.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

UK GDPR / Data Protection Act 2018 Dacorum Borough Council Policy Statement

This is a statement of UK GDPR / Data Protection Act 2018 policy adopted by Dacorum Borough Council.

Dacorum Borough Council needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees, suppliers, client/customers, and others with whom it communicates. In addition, it may be a legal requirement to collect and use certain types of information, for example to comply with the requirements of Government Departments for business data. This Personal Data must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are sanctions to enforce this is in the UK GDPR and Data Protection Act 2018.

The Council regards the lawful and correct processing of Personal Data and Special Categories Data as very important to the successful operation of its services, and to maintaining the confidence of the public. The Council will ensure that it will treat Personal Data lawfully and correctly.

To this end the Council fully endorses and will comply with the ‘GDPR Articles and the Data Protection Act 2018 Clauses.

Scope

This policy applies to all Council employees, councillors, partners, contractors and agents of the Council (i.e. voluntary sector) who process Personal Data and Special Categories of Data or have access to Personal Data or Special Categories of Data in any Council system, files, email, database or manual records.

Definitions

‘Data Controller’ – the legal entity responsible for compliance to GDPR – The Council.

‘Data Processor’ – a natural or legal person, public authority, agency or other body which processed Personal Data on behalf of the Data Controller.

‘Data Protection Act 2018’ - An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner’s functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

‘Data Subject’ – A living individual who is the subject of the Personal Data (e.g. Employee, Resident, Customer)

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31st December 2021	Classification	UNRESTRICTED

'GDPR' - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC as updated, superseded or repealed from time to time.

'Personal Data' - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Special Categories' - Processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

UK GDPR - means the retained UK Law version of the General Data Protection Regulation Brought into effect by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI: 2019 419)

The Principles – Conditions for processing

Article 5 of the UK GDPR requires that the Council process Personal Data in accordance with the following principles.

Personal Data must be;

- (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- (b) 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;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) 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;
- (e) 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

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

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; and;

- (f) 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;

Failure to comply with any of the above principles of UK GDPR will be considered a breach.

Therefore, Dacorum Borough Council will, through appropriate management and strict application of criteria and controls;

- (a) Comply with conditions regarding the fair collection and use of information and establish the lawful basis for processing Personal Data (Article 6 UK GDPR);
- (b) meet its legal obligations to specify the purposes for which information is used;
- (c) collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- (d) ensure the quality of information used;
- (e) apply strict checks to determine the length of time information is held;
- (f) ensure that the rights of people about whom information is held can be fully exercised under the UK GDPR / Data Protection Act 2018 in accordance with the rights set out below.
- (g) take appropriate technical and organisational security measures to safeguard Personal Data (electronic and manual);

Lawfulness of Processing (Personal Data)

Article 6(1) of UK GDPR sets out the following lawful bases for processing;

- The Data Controller has to comply with a legal obligation to which the Controller is subject.
- The processing is necessary for the performance of a contract to which the data subject is a party, or steps prior to entering a contract with a data subject.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

- The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or third party.
- The Data Subject has given their consent to the processing
- The processing is necessary to protect the vital interests of the Data Subject
- The 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.

Individuals Rights

- Individuals have the right to be informed about the collection and use of their Personal Data
- Individuals have the right to access their Personal Data and supplementary information
- Individuals have the right to have inaccurate Personal Data rectified
- Individuals have the right to request their Personal Data to be erased ('right to be forgotten') in certain circumstances.
- Individuals have the right to restriction or suppression of Personal Data (in certain circumstances)
- Individuals have the right to Data Portability
- Individuals have the right to object to processing (in certain circumstances)
- Individuals have the right to object to automated decision making

Subject Access Requests

The Council must process a request for information from a data subject (also known as a subject access request) by 1 (one) calendar month from date of receipt. The Council may request identification from the data subject to confirm the identity of the data subject.

The Council is entitled to request identification under law as set out in UK GDPR Article 12 (6), and we reserve the right to suspend processing a subject access request until we are satisfied as to the identity of the requestor.

This is independent of other departments, and we will require photographic identification such as driver's license, or passport, or any other photographic identity that confirms your address and your name.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

These will be destroyed after a set period when the request has been completed.

A 'reasonable fee' may only be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive, or if further copies of the same information is requested.

Children's Personal Data

When processing personal data of a child aged 13 years (or younger) – parental or guardian consent must be required before processing can take place.

Privacy by Design

The Council is committed to a 'privacy by design and default' approach'; that is the Council will ensure that privacy and data protection is a key consideration in the early stages of any project where the 'rights and freedoms' of people will be significantly affected or where a system is introduced that will affect people's Personal Data. These include but are not limited to; ICT Systems (processing Personal Data), developing legislation, policy or strategies that have privacy implications, data sharing or using data for new purposes.

The Council will conduct privacy impact assessments and include contractual UK GDPR clauses in data processor contracts.

Privacy Notice

The council will publish all relevant privacy notices and ensure they are regularly reviewed and updated. A privacy notice is part of the fair, lawful and transparency principle under Article 5(1) of UK GDPR

Notification

The Council must notify the ICO annually of its record of processing activities. The Council must pay the Tier 3 charge to notify.

International Transfers

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.

Appointment of a Data Protection Officer

In accordance with Article 37(1) – (7) the Council formally appoints a Data Protection Officer (DPO). The DPO reports to CMT and will be a designated duty of the Information Security Team Leader within the Legal Governance Department.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

Other Policy Conditions

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31st December 2021	Classification	UNRESTRICTED

In addition, Dacorum Borough Council will ensure that:

- everyone managing and handling Personal Data understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling Personal Data is appropriately trained to do so;
- everyone managing and handling Personal Data is appropriately supervised;
- anybody wanting to make enquiries about handling personal Information knows what to do;
- queries about handling Personal Data are promptly and courteously dealt with;
- methods of handling Personal Data are clearly described;
- a regular review and audit is made of the way Personal Data is managed, including CCTV systems.
- methods of handling Personal Data are regularly assessed and evaluated;
- regular assessments of our compliance with the GDPR / Data Protection Act 2018 will take place.

Offences

Staff must be aware of the following offences under the UK GDPR / Data Protection Act 2018;

- (1) It is an offence for a person knowingly or recklessly;
 - (a) to obtain or disclose Personal Data without the consent of the controller,
 - (b) to procure the disclosure of Personal Data to another person without the consent of the controller, or
 - (c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the Personal Data when it was obtained.

- (2) It is an offence for a person to sell Personal Data if the person obtained the data in circumstances in which an offence under subsection (1) *{above}* was committed.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

It is an offence for a person to offer to sell Personal Data if the person;

- (a) has obtained the data in circumstances in which an offence under subsection (1) *{above}* was committed, or
 - (b) subsequently obtains the data in such circumstances.
- (3) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified Personal Data without the consent of the controller responsible for de-identifying the personal data.
- (4) It is an offence for a person knowingly or recklessly to process Personal Data that is information that has been re-identified where the person does so;
- (a) without the consent of the controller responsible for de-identifying the personal data, and
 - (b) in circumstances in which the re-identification was an offence under subsection (1) *{above}*.
- (5) It is an offence for a person listed in subsection (6) *{below}* to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.
- (6) Those persons are;
- (a) the controller, and
 - (b) a person who is employed by the controller,

NOTE: This is not an exhaustive list of offences, all offences stated in UK GDPR and Data Protection Act 2018 are relevant to this policy and the persons listed in the scope of this policy.

Other Offences

- a) processing Personal Data without notifying the Information Commissioner (and other offences related to notification);
- b) failing to comply with an enforcement notice or an information notice, or knowingly or recklessly making a false statement in compliance with an information notice.
- c) obstructing, or failing to give reasonable assistance in, the execution of a search warrant;

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

- d) requiring someone, for example during the recruitment process, to exercise their subject access rights to supply certain information (such as records of their criminal convictions), which the person wanting it would not otherwise be entitled to. This offence, known as “enforced subject access”

Compliance

Failure to comply with this policy will result in disciplinary action being taken in line with the Council’s Conduct Procedure. Or, in the case of a councillor, under the Members’ Code of Conduct.

Staff Training

UK GDPR / Data Protection Act 2018 training is compulsory for all staff. New staff must attend the next available training course with a recommendation that current staff should refresh and update their knowledge attending the UK GDPR / Data Protection Act 2018 training course at least once every three years or sooner if there are substantive changes to the legislation.

Reporting a Breach

All UK GDPR, GDPR and Data Protection Act 2018 breaches or suspected must be reported immediately to your line manager who in turn must report the breach to the Information Security Team Leader or the Solicitor to the Council - Legal Governance.

If a breach has been reported to you by a Data Processor. That breach must be reported immediately to your line manager who in turn must report the breach to the Information Security Team Leader or the Solicitor to the Council - Legal Governance.

Further details are provided in the ‘Personal Data Breach or Incident Reporting Procedure’ (DBC999 IS PROC) found on the Council’s Intranet.

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED

Document Control

Author:	John Worts - Information Security Team
Owner:	Mark Brookes – Legal Governance
Document Number	1.5
Full Document Title	DBC100 IM Policy – UK GDPR / Data Protection Act 2018 Policy

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Next Review Date
16 th April 2018	N/A	First Draft	
17 th April 2018	16/4/18	FINAL – Approved by CEO	April 2019
18 th May 2018	17/4/18	Bill to Act (readiness for Royal Assent). Level of fine added	May 2019
24 th May 2018	18/5/18	Changed UK DPA to Data Protection Act 2018. DPA 2018 definition added. Scope changed to include electronic and manual records. Removed fee value.	May 2019
20 th November 2020	24/5/18	Removed ICO Line. Updated CEO	Nov 2020
8 th January 2021	20/11/20	Updated title. Changes to policy conditions	Jan 2022
31 st December 2021	8/1/21	Updates to training and procedure for ID	

Document Approvals

Version	Approved By	Date
0.1	Legal Governance	4/2018
1.0	C.E.O	17/4/18
1.1	Legal Governance	18/5/18
1.2	Legal Governance	24/5/18
1.3	Legal Governance	20/11/20
1.4	Legal Governance	8/1/21
1.5	Legal Governance	31/12/21

Number:	DBC100 IM Policy	Title:	GDPR / Data Protection Act 2018 Policy				
Owner:	AD – Legal, Democratic & Regulatory	Rev	1.5	Date	31 st December 2021	Classification	UNRESTRICTED