DATA PROTECTION POLICY

Contents

1 Definitions

Data Protection Act 2018 ("DPA")	The law on data protection in the UK
General Data Protection Regulation ("GDPR")	A new law on data protection that comes into force on 25 May 2018 throughout Europe
Data Controller	A person or organisation that handles and processes personal data and determines the way such data should be processed
Personal Data	Any information from which a living individual can be identified
Sensitive Personal Data	Any Personal Data which includes further information as defined in the DPA. Further information includes (i) racial or ethnic origin; (ii) political opinions; (iii) religious beliefs; (iv) membership of a trade union; (v) physical or mental health or condition; (vi) sexual life or preferences; (vii) information about any criminal offence or court proceedings related to a criminal offence
Information Commissioner's Office ("ICO")	The statutory regulator of the DPA and the GDPR
Data Privacy Notice ("DPN")	A description of Personal Data held by the Reading Borough Council, along with details of purpose, retention and other information about how the Council will handle the Personal Data
Data Subject	As defined in the DPA and the GDPR. The Data Subject is the person who the Personal Data is about, or who is identified by the Personal Data
Data Privacy Impact Assessment ("DPIA")	A new obligation under the GDPR which requires us to set out and have recorded all our processing activities across the council. It will also help us to identify and tackle data privacy problems at an early stage and ultimately help to reduce associated costs and damage to RBC's reputation
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of data controller.

2 Purpose

This Policy is intended to ensure that Personal Data is dealt with correctly and securely and in accordance with the DPA, GDPR and other related legislation. It will apply to information regardless of how it is collected, used, recorded, stored and destroyed or deleted, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of Personal Data will be aware of their duties and responsibilities by adhering to these guidelines.

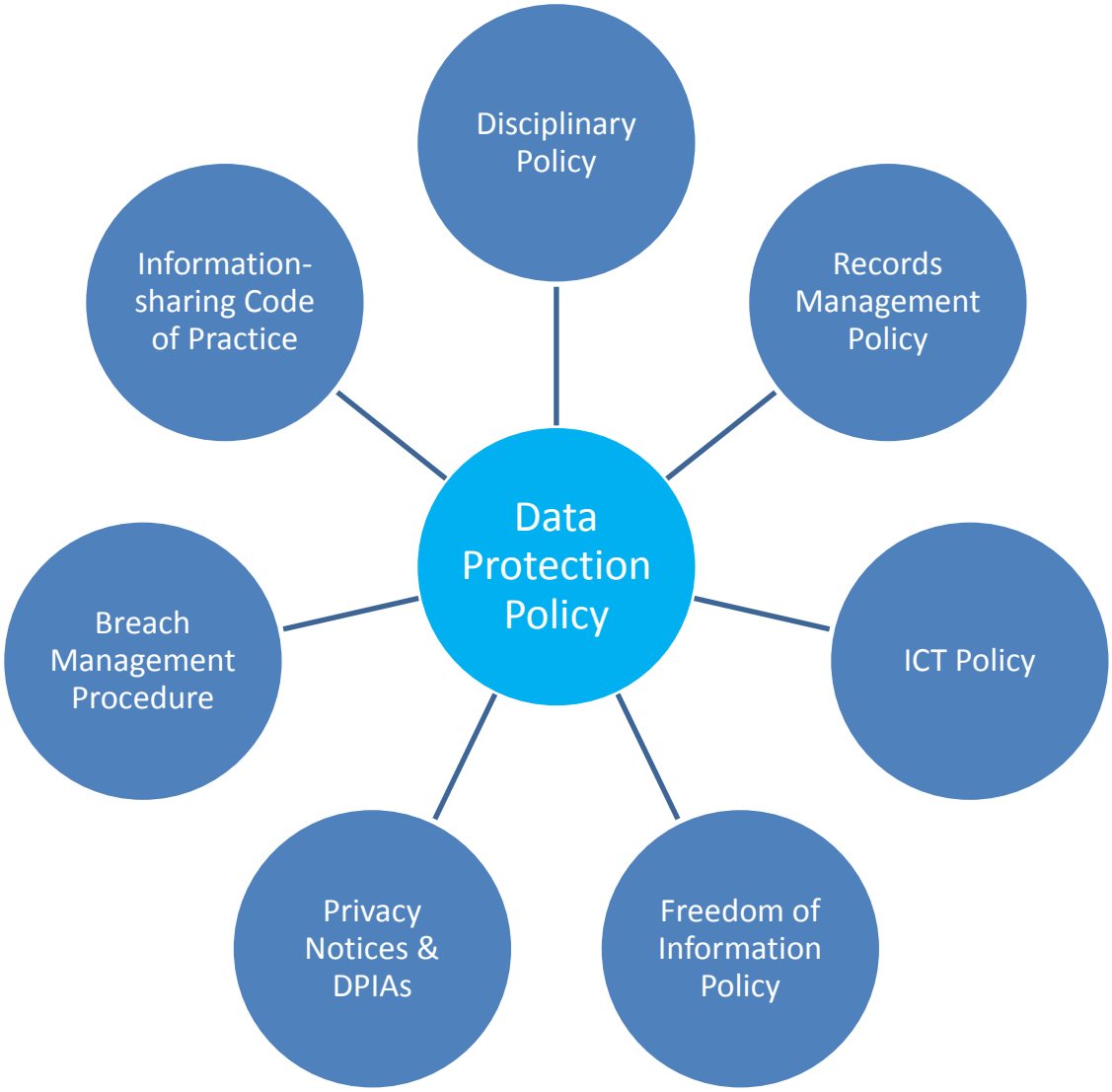
This Policy is central to the Council's suite of policies designed to ensure that the Council is compliant with the DPA in all aspects of its work where Personal Data is handled.

The spidergram overleaf shows how this Policy interacts with those other policies.

Staff are expected to adhere to the principles and spirit of this Policy in order to protect Personal Data belonging to our customers and staff. Anyone found to have breached this Policy may find that the Council will invoke the Disciplinary Procedure.

This Policy has been approved by the Corporate Information Governance Board and is evidence of the commitment the Council makes to safeguarding Personal Data.

3 Spidergram of Policies



4 Data Protection Principles

Article 5 of the GDPR requires that personal data shall 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 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 GDPR in order to safeguard the rights and freedoms of individuals

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.

The Council is committed to maintaining the above principles at all times. Therefore the Council will:

- Inform individuals why Personal Data is being collected and when
- Inform individuals that their information may be shared and why and with whom
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

5 Fair & Lawful Processing

The Council needs to collect and handle Personal Data for a number of reasons.

Customer/Service Users Data

We process personal data of customers and service users in order to provide a service requested by those customers, to safeguard individuals or to provide a statutory service as follows:

- Name, address, date of birth, gender, contact information
- Next of kin and contact details
- Allergies, dietary and medical information
- Ethnic origin
- Any special education needs (SEN)
- Progress data, including national curriculum assessment results, attendance information
- Relevant data from a previous school
- Any safeguarding or social services information, including court information, and adoption status
- Nationality and country of birth
- Immigration status, date of entry to the UK
- Accident records and behaviour
- Financial information
- Criminal conviction data
- Other information as required to enable the Council to provide the service

The Council collects and uses this personal information in order to provide both statutory and requested services.

The Council is required by law to collect and share certain types of information with external bodies such as Local (Education) Authorities (LAs), government agencies (such as the Department of Education, Department for Work & Pensions, Home Office, HM Revenue & Customs) and other bodies to comply with our statutory obligations.

Staff Data

Data is held about staff. This includes

- name, address, phone number, next of kin, emergency contact details
- car insurance details, car registration number
- bank details, earnings from other sources or previous employer, pensions data
- DBS number and date authorised (including spent and unspent convictions)
- medical details, including records of sickness absence and maternity/paternity
- work history, educational history, references
- ethnicity, sexuality, personal living arrangements
- criminal offences/cautions relating to themselves and their partners
- nationality, right to work, and forms of ID (passports, driving licence)
- performance data, disciplinary records

This data is held to enable the Council to comply with its legal obligations and to ensure safeguarding requirements are met.

Parents/ Carers
Data may be held about those with parental responsibility for children for whom a service is provided, whether by request or due to Safeguarding issues. This data includes

- their name, address, emergency contact details, email address, phone number, date of birth
- banking information, income information (if claiming free school meals)
- national asylum support service number (if they're seeking asylum)
- whether they have parental responsibility, and information about injunctions/court orders if applicable

Visitors and others
From time to time, there will be visiting professionals to the Council.

Contractors' details will also be stored. This includes their name, the organisation they work for, a DBS check (or accompanied), car registration number, and contact details.
Other visitors will be required to sign in, thus providing their name and organisation details.

Information consisting of Personal Data may also be shared with law enforcement agencies, such as the Police, from time to time in order to assist them with the prevention and detection of crime.

If we collect data for any other purposes, or from any other person, we will ensure that the purpose of the processing of that data is clear and where necessary, consent is obtained in advance.

Data security
Regardless of the purpose, Personal Data will always be held securely. If in paper format, Personal Data will always be held in secure rooms with access only to authorised individuals. If in electronic format, Personal Data will be stored on encrypted laptops belonging to the Council. No member of staff is permitted to store any Personal Data on unencrypted media or on personal devices.

6 Accuracy of Personal Data

Under the DPA, the Council is required to ensure that Personal Data is kept accurate and up-to-date. To comply with the applicable law, the Council will:

- Take reasonable steps to ensure the accuracy of any Personal Data that is obtained;
- Ensure that the source of any Personal Data is clear;
- Carefully consider any challenges to the accuracy of Personal Data; and
- Consider where necessary if Personal Data needs to be updated or rectified

If a Data Subject informs the Council of a change of circumstances, or notifies the Council of an error, inaccuracy or defect in the Personal Data held, the Council will update both paper and electronic records as soon as practicable. This will normally be done within 20 working days.

Where a Data Subject challenges the accuracy of the data, the Council will immediately mark the record as potentially inaccurate. In the case of any dispute, the Council will try

to resolve the issue informally but if this is not successful, disputes will be referred to the Corporate Information Governance Board for a decision.

7 Retention Periods

This section sets out a framework for management decisions on whether a particular document (or set of documents) will either be:

- Retained – and if so in what format and for what period
- Disposed of – and if so by when and by what method

Data retention periods can be found at the following link:

http://inside.reading.gov.uk/myhome/infopods/informationgovernancepod/

All other Personal Data falling outside of these periods will be securely destroyed.
All records that are to be retained will be retained securely.

Destruction of records
Where paper records are identified as needing to be destroyed, these will be shredded securely by the relevant provider procured by the Council. Currently destruction of records takes place onsite using shredders.

8 Information Rights

a. Subject Access Requests (SARs)

A customer, or someone acting on their behalf, may make a Subject Access Request in respect of Personal Data held by the Council.

The SAR process can be found at the following link:
http://inside.reading.gov.uk/myhome/infopods/informationgovernancepod/

The SAR form can also be found at Appendix A of this policy.

b. Right to be forgotten

Under the GDPR, individuals have the right to request the Council to delete Personal Data where there is no compelling reason for them to retain it:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

An individual may make a request by writing to the Information Governance Team if they wish to request the Council delete or remove any Personal Data. The Council will consider such a request and within 30 days will either confirm the deletion or removal of all Personal Data (other than retaining a record of the request itself) or will inform the

individual that the Personal Data will not be deleted, because it is required for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

9 Information Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality
means that only people who are authorised to use the data can access it

Integrity
means that personal data should be accurate and suitable for the purpose for which it is processed

Availability
means that authorised users should be able to access the data if they need it for authorised purposes- personal data should therefore be stored on the relevant Council computer system instead of individual PCs

Security procedures include:

- Entry controls
  Any stranger seen in entry-controlled areas should be reported

- Secure lockable desks and cupboards
  Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential)

- Methods of disposal
  Paper documents should be shredded
  Records stored on digital storage devices should be destroyed when they are no longer required

- Equipment
  Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

10 Training & Development

The Council is committed to ensuring the staff adopt the highest standards in relation to the processing and handling of Personal Data.

Face to face Data Protection refresher training is available to staff and staff are expected to complete it.

New staff will be expected to complete the Introduction to GDPR E-Learning module as part of their induction training.

Staff will be re-trained according to their needs against the tide of new guidance and legislation. It is anticipated that this will usually be annually.

Members of staff are expected to read this policy.

11 Further Information

Any person reading this Policy requiring further information or assistance is invited to contact the Data Protection Officer or the Information Governance Team.

Where any person has a complaint about the way the Council has handled their Personal Data or that of their child's, they may address their concern in writing to the Data Protection Officer.

For further information about the DPA, GDPR and its application, the Information Commissioner's Office has a wealth of information on its website – www.ico.org.uk

APPENDIX 1

READING BOROUGH COUNCIL

SUBJECT ACCESS REQUEST FORM

General Data Protection Regulation – SUBJECT ACCESS REQUEST

Please provide the following details about yourself:

Full name .....

Address.....

Tel No ....

E-mail: .....

Previous addresses in Reading (where appropriate).....

.....

.....

.....

1.Are you requesting information about yourself?

If so, you are the applicant and documentary evidence of your identity is required, i.e. driving licence, birth certificate (photocopy) and a copy of a recent utility bill. Please complete sections 2, 3 and 6 below.

If not, you will need to supply the written consent of the applicant on whose behalf you are acting and complete sections 3, 4, 5 and 6 below.

---

2. Please describe the information you seek together with any other relevant information to help us identify the information you require.

.....

.....

.....

3. To help us locate any personal information which we hold, please tick the relevant subject box below

Education (e.g. Student Support and Admissions, Education Welfare, Education Psychology, Special Education, Children & Families Services, Governor Services, School Transport) ☐

Leisure Services (e.g. Arts, Countryside & Heritage, Sports & Recreation, Libraries) ☐

Planning & Transportation (e.g. Planning Applications & Development Control Parking) ☐

Public & Environmental Services (e.g. Public Health, Refuse Collection, Waste Disposal, Trading Standards) ☐

Community Care & Housing (e.g. Housing, Housing Benefits, Housing Repairs, Social Services, Youth Offending) ☐

Corporate Services (e.g. Council Tax, Land Charges, Registration of Births, Deaths and Marriages, Elections and Electoral Registration, Personnel ☐

---

4. If you are you authorised to act on behalf of the applicant, please complete the following

Details of applicant on whose behalf you are acting

Full name .....

Address .....

.....

Tel No .....

E-mail: .....

Relationship to the applicant .....
(eg parent, guardian, social worker, solicitor etc)

Please briefly explain why you are requesting this information rather than the applicant.

.....

.....

.....

5. The applicant on whose behalf you are acting must complete the following authorisation

I .....(Name of person on whose behalf application is made) authorise ....(Name of person making the application) to seek access to personal information held by Reading Borough Council. I declare that this authorisation was freely given.

Signed ..... Date .....

---

6 ALL APPLICANTS MUST COMPLETE THIS SECTION [Please note that any attempt to mislead may result in prosecution].

I ..... confirm that the information given on this application form to Reading Borough Council is true, and I understand that you may need more information to confirm my identity/that of the data subject and to locate the information that I am requesting.

Signature: .....

Date: .....

Please return the completed form to the Data Protection Officer, Legal Services, Reading Borough Council, Civic Office, Bridge Street, Reading, RG1 2LU, along with **photocopies** of your evidence of your identity or by email to sarrequests@reading.gov.uk.