Data Protection Rights Policy

1. Purpose

This policy outlines the standards expected of all Brighton & Hove City Council employees, and any third party processors holding personally identifiable information on behalf of the Council when responding to residents, staff and others seeking to exercise the various Data Protection rights established under GDPR.

This is a public facing policy which is intended to establish what people seeking to exercise their data protection rights should expect from the Council and its partners.

2. Targeted Audience and Scope

- Employees of Brighton & Hove City Council
- Organisations commissioned by BHCC and their staff
- Service delivery partners and their staff
- Residents of the city and other data subjects

3. Background

In May 2018, a new data protection regulatory framework (the GDPR) came into force. This has subsequently been supplemented by the Data Protection Act 2018. Both the GDPR and the 2018 Act have legal force in the United Kingdom.

The new law significantly expands the rights which people have with regard to the personal information about them held by organisations. The Information Commissioners' Office ('ICO') has the power to issue proportionate and dissuasive fines of up to £16,000,000 for failure to comply with data subject rights

4. Definitions

- Data Controller – The organisation which either individually or jointly decides the purposes and methods of data processing.

- Data Processor – An organisation which processes data on behalf of the data controller

- Data Subject – The person the data is about

- Legal basis – The principle or principles under which it is permissible for the Council to use particular data about somebody

- Personal Data – Any information relating to a living person who is directly or indirectly identifiable which is processed by computer.
  Processing – Any action taken which uses personal data

- Special Category Data – data relating to a person's race, ethnic origin, politics,

religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

5. The Data Protection Rights

Which rights someone can exercise over the data organisations hold about them depends to some extent on what the legal basis is for the collection and use of the data.

5.1. The Subject Access Right

The subject access right is the right for people to know whether an organisation holds data about them and what it is used for. This right is important as the ability for people to exercise the rest of their data protection rights largely hinges on them being able to be informed about what data there is and what it is used for. Upon receiving a subject access request, and unless an exemption applies, the Council is obliged to inform the requestor as to:

- Whether their personal data is being processed
- The purposes for the processing
- The categories of personal data being processed
- Where data was obtained from someone other than the requestor, the source of the data
- Of the categories of recipient to which the data has or will be disclosed
- Where possible, the envisaged time period for which the data will be kept, and if this is not possible, a description of the criteria used to determine how long it is kept.
- Which other data protection rights exist regarding the use of this data
- The existence of the right to complain to the Information Commissioner's Office
- Whether or not decisions are being made by an automated/computerized process and (if so) an explanation of the logic behind those decisions

The Council must also provide a copy of the data held or any portion of that data which the data subject requests. This copy should be provided in a form accessible to the data subject, including commonly readable electronic formats where requested

5.2 Guidance for subject access requestors

- The subject access right is not absolute. There are constraints and exemptions which apply in certain circumstances. Where an exemption is applied, the council will endeavor to be transparent about which one and the reasoning behind it, but there are some cases where this cannot be lawfully done.
- Subject access requests may only be made by the data subject, someone with lawful guardianship or someone with power of attorney
- Whilst requests from parents for data concerning their children will be respected if it can be shown that they are exercising the right on behalf of their child, parents do not have an automatic right to the data about their children. Requests by parents may be refused if in the opnion of specialist staff working with the children, it would not be in the interests of the child to disclose the data and subject to relevant exemptions.
- Subject access requests are not required to be made in writing, but the Council provides a form on its website which requestors may use if they wish to.
- The Council is required to provide a response to a subject access request within one calendar month. This may be extended for up to a further two months in complex cases. Where an extension of the 30 days will be required, the Council will inform

the requestor of this as soon as practicable and in any case prior to the expiry of the one month deadline.

- Where necessary, the Council will seek to verify the identity of the requestor prior to processing the request. If a requestor's identity cannot be established, the request cannot lawfully be processed.

6. Further Information Rights

The Data Protection Act 2018 provides for further data subject rights, which are set out below. If someone is not clear on what data is held or used by the Council, are advised to make a subject access request I order to understand what data is held and whether they wish to exercise other rights.

Data subjects can submit requests for any of the these rights by emailing data.protection@brighton-hove.gov.uk or by calling 01273 295959

6.1 Right to Rectification (Correction) of Data

This is the right to have corrected any data held which can be shown to be not correct. It recognises that poor data leads leads to poor decisions and actions, which may unfairly effect someone's life.

Upon receipt of a request to rectify data, the Council is obliged to consider whether it should be changed and to provide a response to the requestor. The Council will not change the data in the following circumstances:

- If the Council believes that the data is correct

- Where the Council is obliged by a law or regulator not to change the data

Where the Council is unable to change the data it holds in response to a request, it will provide a clear written explanation as to why it has not done so. In these cases, a requestor may be offered the opportunity to place a statement on the record concerning the matter.

6.2 Right to Erasure

The right to erasure is commonly referred to as the right to be forgotten. Requests for data to be erased must be respected by the Council if any of the following circumstances apply:

- Data was collected on the basis of consent and there is no other legal basis on which to hold it

- The data was collected on the basis of the legitimate interests of the Council and either this legitimate interest no longer exists, or is outweighed by the right to privacy

- The data is found not to be lawfully held

Upon receipt of a request for erasure, the Council will consider which legal bases for collection apply and whether the data can be deleted. If that data cannot be deleted, the Council will provide a response explaining the legal basis for processing and why the data may not be erased. If it is possible to do so, the Council will provide an explanation as to when and under what circumstances it is likely to be able to erase the data at a future

time.

6.3 Right to Restrict Processing

The right to restrict processing can be used in any of the following circumstances:

- If a data subject has made a request to rectify their data, the use of that data may be restricted until this request has been assessed and responded to. However, this does not apply where the Council is legally obliged to process the data.

- If a data subject has raised an objection to processing (see 7.4) and the Council is still considering its response to that.

- If it has been shown that the Council has been processing the data without a legal bais to do so and the data subject requires that the data is not deleted, perhaps so that they can consider taking legal action.

6.4 Right to object to processing

Data subjects may make an objection to processing where the Council's legal basis for the processing is either:

- A task in the public interest
- The legitimate interests of the Council

Upon receipt of an objection to processing, the Council is obliged to cease using the data unless (and until) it can provide a compelling justification for why the lawful basis for the use of the data overrides the privacy interests of the data subject.

6.5 Right to object to automated decision making

Data subjects have a right to object to automated decision making and insist that the decision be made by a human being.

The Council has very few examples where automated decision making occurs and is obliged to disclose such instances to data subjects via privacy notices.

6.6 Right to portability

Data subjects have a right to have their data transferred in a commonly accessible format to other organisations where the lawful basis for holding it was either consent or performance of a contract.

In other cases, where there is a public interest in transferring data to another organisation (such as another Local Authority), the Council will take reasonable efforts to comply with a data subject request that it do so.

7. Roles and Responsibilities

- The Information Governance Team is responsible for central logging of data protection rights requests, allocation of these to departmental coordinators and provision of data protection advice to staff tasked with handling the matter

- Information Asset Owners are responsible for assuring that there are adequate local procedures and resources to enable effective handling of the requests, that the legal basies for processing of all personal data is recorded on Information Asset Registers and that these are also transparent to data subjects through privacy notices.

- Team and line managers are operationally responsible for ensuring requests allocated to their team are complied with in accordance with the approved departmental procedures

- The Information Governance Board is responsible for reviewing and advising on this policy, consideration of high level organizational impact and risks and making recommendations to the Senior Information Risk Owner

- The Senior Information Risk Owner is the owner of this policy and accountable for organizational performance against it

- All staff are responsible for adhering, reading and understanding this policy. They must also make sure that any data protection rights requests are forwarded to the Information Governance Team for logging

8. Process for People Exercising the Data Protection Rights

Requests on data protection rights should be made to the Data Protection Team by emailing data.protection@brighton-hove.gov.uk or by telephone on 01273 295959

- If you do not know what data is held, it is recommended that you first make a subject access request
- If you already have a copy of the data you are concerned about, please provide it to the Data Protection Team along with an explanation for the right you wish to exercise

9. Training Requirements

- As a minimum all staff are required to complete Information Governance E-Learning on an annual basis

- This must be supplemented with training in local procedures relevant to data protection rights relevant to the service staff work in

10. Risks

Brighton & Hove City Council recognises the risks associated with users handling information in order to conduct official Council business.

A failure to respond appropriately to a data protection rights request may result in legal action against the Council (as the Data Controller) and/or disciplinary consequences for the employee concerned

Non-compliance with this policy may result in damage or distress to an individual/individuals, financial loss, compromise our ability to provide services to our customers and/or cause damage to the Council's reputation.

The Information Commissioners' Office ('ICO') has the power to issue fines of up to £16,000,000 for failure to comply with data subject rights

11. Review of this Policy

This policy will be reviewed annually.

12. Cross References

Data Protection Policy
Information Sharing
Policy
Data Quality Policy

13. References

Data Protection Act 2018
The General Data Protection Regulation
Regulation of Investigatory Powers Act 2000

14. Policy Control Details

Policy Name	Data Rights Policy
Document Type	Public Facing Policy
Version	1.0
Introduction Date	23 February 2019
Effective Date	23 February 2019
Next Review Date:	23 Feburary 2020
Reviewed by:	Information Governance Board
Approved by:	Executive Director of Finance and Resources
Document Author	Data Protection Manager
Document Owner	Senior Information Risk Owner

Please find all Information Governance policies here.