Data Protection Rights Policy

1. Purpose

This policy outlines the expectations of staff, contractors and partners tasked with responding to data subject rights requests made under the UK (United Kingdom) General Data Protection Regulation and Data Protection Act 2018.

This is a public facing policy which is intended to assist people by outlining the several types of rights requests, the circumstances in which they can be exercised and what to expect.

2. Targeted Audience and Scope

- Council Members
- Employees of Brighton & Hove City Council
- Organisations commissioned by BHCC (Brighton & Hove City Council) 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 (General Data Protection Regulation)) came into force in British law. At the same time, the Data Protection Act 2018 came into force, codifying and clarifying aspects of the GDPR.

Subsequently, at the time of exit from the EU, the UK GDPR was passed, placing the entirety of the GDPR in national law.

The new legal framework significantly expands the rights of people about the personal information about them held and used by organisations. There are now criminal penalties for egregious contraventions and 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

- GDPR – The General Data Protection Regulation which was brought into UK law as a regulation of the EU parliament. The Data Protection Act 2018 was passed to bring the mandatory elements of GDPR into UK law in anticipation of Brexit.

- Lawful basis – The criteria set out in Article 6 and 9 of the GDPR, setting out the

circumstances under which it is legal to collect, use and/or share somebody's personal data

- 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

Under the GDPR, data subjects can make six distinct types of rights requests. However, not all of them apply in all circumstances. Which rights are applicable depends upon what lawful basis for processing of data is applicable. The table below sets out which rights can be exercised and under what circumstances:

		How does your Lawfulness of Processing impact your ability to execise your individual rights?					
	Note all these rights are subject to exemption within the Data Protection Act						
Individual Rights / Lawfulness of Processing	Right to Erasure	Right to Portability	Right to Object	Right to Rectification	Right of Access	Right to be informed	Right to Restrict Processing
Consent	✓	✓	✗	✓	✓	✓	✓
Contract	✓	✓	✗	✓	✓	✓	✓
Legal Obligation	✗	✗	✗	✓	✓	✓	✓
Vital Interest	✓	✗	✗	✓	✓	✓	✓
Public Task	✗	✗	✓	✓	✓	✓	✓
Legitimate Interest	✓	✗	✓	✓	✓	✓	✓

5.1. The Subject Access Right

The subject access right is the right for people to know whether an organisation holds data about them, what that data is, where it came from 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 informed as to how and why their data is collected and used. Upon receiving a subject access request, unless there is a specific statutory exemption, the Council is obliged to inform the requestor:

- 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
- 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 if the data subject believes their rights have been contravened.

- 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. The data should be provided in a form accessible to the data subject, including commonly readable electronic formats if these are requested and if it is technically feasible to produce the data in this form.

It should be noted that where data is required to be shared with a service user through operational practice, the person should not be directed to make a subject access request.

5.2 Guidance for subject access requestors

- The subject access right is not absolute. There are a range of exemptions which apply in certain circumstances. Wherever possible, the Council will be transparent about which exemptions were applied and the nature of any material withheld from disclosure. However, it may not be able to do this if doing so would contravene another person's rights or put them at risk.

- Subject access requests may only be made by the data subject themselves, someone with a formal guardianship relationship or by someone with written authority to act for the data subject.

- Parents do not have an absolute right to access data about their children. Upon receipt of a request from a parent for data about their child, the Council is required to assess whether the parent is acting in the child's interests or acting on their own behalf.

- 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 form may help requestors to focus their request.

- 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 is 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.

- If the identity of the requestor cannot be verified in any other way, the Council will require the provision of identification. If a requestor's identity cannot be established, the request cannot lawfully be processed.

- Requestors are advised to read the Frequently Asked Questions from the Information Commissioner's Office if they wish to better understand their rights and what they can expect from the SAR (Subject Access Request) process.

  https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Data subjects can submit requests for their information by emailing dsar@brighton-hove.gov.uk, writing to or by calling 01273 295959. Alternatively, they can be sent by post to;

Information Rights Team
Brighton and Hove City Council
Room 233
Hove Town Hall
Norton Road
Hove
BN3 3BQ

6. Further Information Rights

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

Data subjects can submit requests for any of these rights by emailing data.protection@brighton-hove.gov.uk or by calling 01273 295959. Alternatively, they can be sent by post to;

Information Rights Team
Brighton and Hove City Council
Room 233
Hove Town Hall
Norton Road
Hove
BN3 3BQ

6.1 Right to Rectification (Correction) of Data

Data subjects have the right to seek correction of any data held about them that is objectively incorrect. This is not a right to change history. Sometimes the council will receive data (such as a safeguarding referral) which subsequently does not turn out to be correct. In these circumstances, the fact of the data and the decisions/actions taken in response cannot be altered.

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:

- Where, upon reflection, the Council considers that the data is correct
- Where the Council is obliged by a law or regulator not to change the data, such as data associated with performance of social care functions.

In cases where the Council is unable to change the data it holds in response to a request; it will provide the requestor with a clear written explanation as to why it has not done so.

In cases where data cannot be changed, the data subject should be offered the opportunity to place a statement on the record concerning their own views of the matter at hand and how these differ from the Council's record.

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:

- The data is no longer necessary for the purpose it was originally collected or processed for.

- Data was collected based on consent, which has now been withdrawn and there is no other lawful basis to hold it

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

- The data is found not to be lawfully held

- The data was formerly lawfully held at one point, but that lawful basis is no longer applicable

Upon receipt of a request for erasure, the Council will consider which legal bases for data processing apply and whether the purposes for data processing are still in place.

Following this, a decision will be made as to whether the data can be deleted or must be retained for a period. If that data cannot be deleted, the Council will provide a response explaining the lawful 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 considering its response to that.

- If it has been substantiated that the Council does not have a lawful basis for processing the data, but the data subject wishes it to be retained whilst they consider their legal options.

6.4 Right to object to processing

Data subjects may make an objection to processing where the Council's lawful 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 (solely by automated means without any human involvement) and insist that the decision be made by a human being.

The Council conducts extremely limited automated processing and discloses all instances of this via its privacy notices.

Data subjects are advised to read the privacy notices for all Council services they have or have had involvement with, if they wish to understand whether they are subject to automated decision making.

6.6 Right to portability

Data subjects have a right to have their data transferred in a commonly accessible format to other organisations that they have provided to the controller 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 make reasonable efforts to comply with a data-subject request that it does so.

7. Roles and Responsibilities

- The Information Rights Team is responsible for central logging of data protection rights requests, allocation of these to departmental coordinators, development of guidance and provision of data protection compliance advice to staff involved in handling of these requests

  Following a decision of the Executive Leadership Team in 2019, the Information Rights Team also centrally processes all subject access requests related to children's social work. All other rights requests relating to children's social work data remain the responsibility of the children's social work department.

- The Information Rights Lead is responsible for the effective management of the Information Rights Team, production of management information concerning risks and performance for the Data Governance and Insight Steering Group, assuring the Data Protection Officer (DPO) and SIRO (Senior Information Risk Owner) are made aware of any serious contraventions of the data protection rights and leading on the response to Information Commissioner casework.

- The Data Protection Officer (DPO) is accountable for exercising oversight over the wider data protection function at the council and provision of expert advice to the Data Governance and Insight Steering Group and SIRO. Requestors may escalate their cases to the Data Protection Officer if they do not consider that the Council has been compliant with the law in its responses.

- Information Asset Owners are responsible for assuring that there are adequate local procedures and resources to enable effective handling of the requests received, that the legal basis for processing of all personal data is recorded on Information Asset Registers and made 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. They are also responsible for deciding what response

to make to requests, taking advice from the Information Rights Team as appropriate.

- The Data Governance and Insight Steering Group is responsible for reviewing and advising the SIRO on this policy as well as assessment of risks and performance arising from processing of rights requests.

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

- All staff are responsible for recognising GDPR rights requests when one is received from a resident or customer and for signposting to the data protection team to ensure that a timely response is made. Where tasked by line management to do so, they are responsible for searching for information within the scope of the request.

8. Process for Exercising the Data Protection Rights

To raise a subject access request, contact should be made to the Information Rights Team by emailing DSAR@brighton-hove.gov.uk

For all other GDPR rights requests, contact should be made to data.protection@brighton-hove.gov.uk

Telephone enquiries can be made by calling 01273 295959

Alternatively, they can be sent in by post to;

Information Rights Team
Brighton and Hove City Council
Room 233
Hove Town Hall
Norton Road
Hove
BN3 3BQ

9. Training Requirements

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

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

- IG Coordinators and IAO's may seek enhanced data protection training in line with their role

- All Information Rights team members have relevant training in line with their role

10. Risks

Brighton & Hove City Council recognises the risks associated with users handling information 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 £17,500,000 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
Information Rights Procedure

13. References

Data Protection Act 2018
The UK General Data Protection Regulation (GDPR)
Regulation of Investigatory Powers Act 2000

14. Policy Control Details

Policy Name	Data Rights Policy
Document Type	Public Facing Policy
Version	4.0
Introduction Date	23 February 2019
Effective Date	01 February 2024
Next Review Date:	01 February 2025
Reviewed by:	Data Governance and Insight Steering Group
Approved by:	Assistant Director (Customer, Modernisation and Performance Insight
Document Author	Information Rights Development Manager
Document Owner	Information Rights Lead