

Subject Access and Data Protection Requests Procedure

Revision History

Version	Date	Summary of Changes	Author
0.1	March 2018	Initial draft	Jaimie Taylor
0.1	April 2018	Draft for approval to IGG	JT
1.0	3 April 2018	Final version	JT
1.1	26 February 2024	Initial review	Jenna Paterson
1.2	27 February 2024	2 nd Check	Nicola Driver
1.3	27 February 2024		JP
1.4	28 February 2024		Gillian Laing
1.5	1 March 2024		JP
2.0	7 March 2024	Final version	JP
3.0	September 2024	Final Version	Nicola Driver

Contents

Introduction 3

 Subject Access Requests 3

 Other rights afforded to individuals 3

Roles & Responsibilities 4

 The Subject Access Request Process 5

 Proof of Identity 5

 Personal Applications: 5

 Written Applications: 6

 Responses: 6

 Complaints..... 6

 Extending the timeframe..... 7

 Charging..... 7

 Requests for children’s personal data 7

Other Data Protection Rights..... 9

Appendix 1 - SAR Distribution Template..... 10

Appendix 2 - SAR Form 12

Appendix 3 - Information Sheet for the Public 15

Introduction

Subject Access Requests

A (living) person has the right under the UK General Data Protection Regulation to request information held about them by the Council. This right is also enshrined in the European Convention on Human Rights which safeguards an individual's right to a private life and respect for personal data under Article 8 and the right to access information under Article 10. This right is known as a Subject Access Request (SAR). If a request is made verbally there is an expectation that advice and assistance will be provided to the individual to enable them to make a valid request. The legislation stipulates that valid requests must be responded to within 30 calendar days.

It is important to note that the request does not need to state that it is a subject access request or mention Data Protection. It may even cite other legislation like the Freedom of Information Act. It is the responsibility of the Council to recognise the request as a SAR and manage the request appropriately. Whilst it can be helpful for the Council to know, there is no requirement for the individual to explain why they are making the request.

Other rights afforded to individuals

Data Protection also provides individuals the right to object; restriction; rectification; erasure and portability. As with Subject Access Requests, each valid request should be fully considered and responded to within 30 calendar days.

Any request received should follow the process described in this guide and be passed to the Information Management Team for validating and logging purposes.

Data Protection is regulated by the UK Information Commissioner (ICO) and should not be confused with the Scottish Information Commissioner (SIC) who regulates the Freedom of Information Act (Scotland) 2002 and the Environmental Information (Scotland) Regulations 2004.

The Information Management Team works closely with the Legal department and is on hand to provide advice and assistance to anyone tasked with responding to a Subject Access Request. Please email dataprotection@scotborders.gov.uk

This guide should be read in conjunction with the [Subject Access Request guidelines](#) available on the Intranet.

There is further advice and guidance available on the [Information Commissioner's website](#)

Documents that may be of particular help are:

[The ICO Right of Access](#)

[The ICO determining what is personal data](#)

Roles & Responsibilities

Although all employees share responsibility for complying with Data Protection law, there are certain responsibilities assigned to officers in specialised roles. The roles are as follows:

Data Protection Officer (DPO)/ Senior Information Risk Officer (SIRO)

The Senior Information Risk Officer maintains overall responsibility for information governance within the Council. The Data Protection Officer provides assurance to senior management and advice on data protection matters. Nuala McKinlay, Director of Corporate Governance, fulfils both roles within the Council.

The Information Management Team

The Information Management Team provides advice and assistance on a range of information governance matters and drives compliance with data protection and associated laws. The team's Information Officers are responsible for providing advice and assistance, validating subject access requests, and providing employees with appropriate guidance on responding to these requests.

Data Protection Coordinators

Each department must also identify a data protection coordinator who will organise their department's response to any individual right request circulated by the Information Management Team. They must ensure that individual right requests are dealt with appropriately and promptly by the services and departments they represent. The coordinators must ensure that these requests are sent to all those within their service who may hold relevant information.

Director

The Director (or delegated officer) of the department providing information in response to the request must carry out a quality assurance check and ensure that the requester receives all the information they are entitled to, and any redactions are in accordance with data protection law. Information cannot be released to the Information Management Team without the appropriate approval.

Legal Team

The Legal Team support the Information Management Team in their role as coordinators and advisors on information governance as and when required.

SAR Advice Group

The group is made up of the Data Protection Officer, Solicitor, and an Information Officer. The group's role is to review and consider the Council's response to SARs in which the requester has stated that they are dissatisfied with the information received for any reason such as the information recorded is inaccurate, unlawfully retained, heavily redacted etc. The service representative and coordinator will be asked to attend a meeting to discuss the request and help inform the group's response to the data protection complaint.

The Subject Access Request Process

Compliance with Data Protection legislation is essential, but it is also imperative that a data subject has access to their personal data in a simple manner and reasonable timescale (within a maximum of 30 calendar days).

Proof of Identity

1. The Act puts the onus on the Council to ensure that the personal data is only disclosed to those who are entitled to have access, and the procedures in force are for the protection of personal data and are not intended to discourage authentic enquiries. The Council must be satisfied that the name and address quoted on the request are genuine, accurate and up to date prior to any disclosure or confirmation of data. Where the request is made by someone acting on another person's behalf e.g., a solicitor, they should be asked to provide a signed letter from the data subject giving them the authority to make such a request. An exemption to this is with Social Work records as they operate an open access policy whereby the client is kept informed of what is happening with their case. Where someone has been granted power of attorney over another person's written affairs, they should produce a copy of the written (enacted) power of attorney evidencing that they have welfare rights.

Personal Applications:

2. Requesters visiting any of the Council's offices should be reassured by staff that the Council understands the importance of Data Protection legislation and wishes to make the subject access request process as simple as possible.
3. If requesters require access under the provisions of the legislation, they should be given an application form (the Council's Subject Access Request Form – Appendix 2), and a copy of the Council's Subject Access Guidance Notes (Appendix 3), and advise a response will be sent to them within thirty calendar days counted from the date on which the Council has sufficient information to identify the personal data concerned.
4. The purpose of the form is to help the requester to provide sufficient information to enable their personal data to be identified. If a requester is unable or unwilling to complete the form the staff member should support the requester to make a valid request or contact an Information Officer to help.
5. The requester should identify where possible which specific applications and / or services they believe the Council holds personal data on them to enable the Council to retrieve the information within the allocated period.
6. If requesters wish to fill the form in at the time of requesting the form, they can do so.
7. The requester may wish to take the form away and can thereafter apply by email to dataprotection@scotborders.gov.uk or by post to the Information Management Team, SBC Headquarters, Newtown St Boswells, TD6 0SA.
8. All completed forms, associated documentation, should be scanned and forwarded immediately to dataprotection@scotborders.gov.uk. The email should be protectively marked with 'Official-Sensitive.'

Written Applications:

9. All written applications should be immediately forwarded to dataprotection@scotborders.go.uk for logging and action. The documentation should be protectively marked with 'Official-Sensitive.'

Responses:

10. The Information Management Team should ensure that all subject access requests are fully responded to within the time limit set down by the legislation.
11. On receipt of a subject access request, the Information Management Team will record the identity of the requester, the date the request was initially received and determine which department(s) should be able to provide the relevant information.
12. Thereafter, an e-mail will be sent to the relevant subject access coordinator. The email, including any attachments, should be protectively marked with 'Official-Sensitive.' Where copies of documentation need to be shared, additional security measures and other methods of sharing should be considered e.g., client copy watermark, use of access-controlled SharePoint folder.
13. As soon as practicably possible, each subject access coordinator(s) will arrange to produce (and where necessary, annotate) in a timely manner a copy of the data subject's personal data held as well as any paper records to ensure that requests are responded to within the time limit. The email, including any attachments, should be protectively marked with 'Official-Sensitive.' Where copies of documentation need to be shared, additional security measures and other methods of sharing should be considered e.g., client copy watermark, use of access-controlled SharePoint folder.
14. Where information has been provided by another organisation, they should be informed where possible and given the opportunity to highlight any concerns or issues with disclosure of the information. If concerns are raised, that organisation needs to explain what exemption they believe applies to this case and what the impact could be on the requester if disclosed at this time. A deadline for responding should be given and should not delay the response to the requester.
15. Once collated, the coordinator should review, taking into account instructions from services and carry out consistent redaction, removing duplication where possible. Coordinators must ensure services complete the search template – this information may be included to help inform response or complaints. A response and information should be passed to the appropriate Director, in a secure manner, for quality assurance and approval. When approved the coordinator should securely share with the Information Management Team.
16. Copies of the requester's personal data should be sent electronically, protectively marked and password protected, however if it requires to be sent by post, it should be sent by recorded delivery by the Information Management Team to an address which can be identified by the requester. The information should be placed in a double envelope and protectively marked. If no data is held, this is still a disclosure of personal data, as such an email/letter stating this should be securely sent to the requester.

Complaints

17. If a requester should be dissatisfied with the Council's response to their subject access request, they are entitled to ask the Council to review its response. The Information Management Team will acknowledge and log the complaint. The team arrange for the SAR Advice Group to meet and consider the complaint. Officers involved in the collation of the information (stated on the search template – see appendix 1) will be asked to attend the meeting. Officers should give priority to this meeting.

18. A minute of the meeting will be taken by an Information Officer, or a Legal Assistant, and a letter will be sent to the requester detailing the group's findings from the Data Protection Officer.
19. The Council will always attempt to address concerns internally however a requester, if still dissatisfied can then appeal to the UK Information Commissioner Office (ICO).

Extending the timeframe

20. The statutory timeframe of 30 days can be extended by up to a further 60 calendar days for cases where the information is both complex and voluminous. This cannot be purely due to record management issues; it should be a task that any organisation would find challenging to undertake.
21. The requester must be informed within 30 calendar days from when the request is validated.

Charging

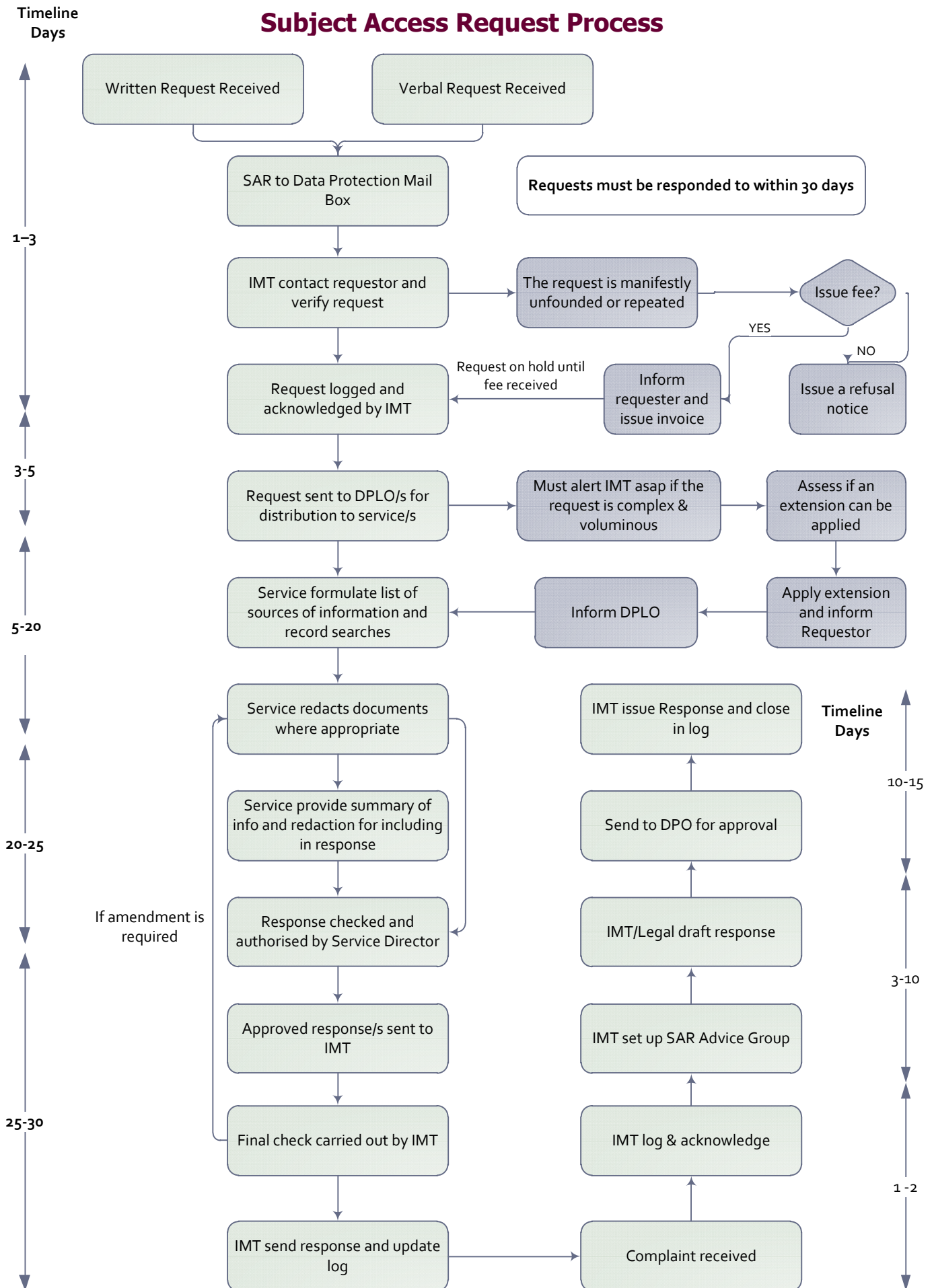
22. Information provided in response to subject access requests should be provided free of charge. However, if the Council concludes that the request is manifestly unfounded; excessive or a repeat, a fee can be charged but it must be reasonable and only take into account the administrative costs of providing the information.
23. If a service wishes to issue a fee, they should discuss with the Information Management Team as soon as possible. If agreed, the requester will be informed and issued with an invoice. The request will be placed on hold until the fee is paid in full.
24. The Council can refuse to comply with a request if it is considered to be manifestly unfounded. This means that it must be obvious that the request has no basis or evidence of contact with the requester, or it is a repeat request. However, this is a high test, and the Council must be able to demonstrate and evidence why it believes the request to be so.
25. As previously stated, if the request is to be refused the Information Management Team should be informed as soon as possible.

Requests for children's personal data

26. In Scotland, a child aged over 12 is deemed to have sufficient capacity to understand their rights over their personal data. Therefore, further consideration should be given to requests received from parents or guardians wishing to access their child's personal data. If the child concerned is under the age of 12, the information can be provided to the parent once it is confirmed that the parent/guardian has parental responsibility for the child. Social Work, if involved with the child or the child's school should be able to confirm this or the parent should be asked to provide a copy of the child's birth certificate along with proof of their identify following the steps described above.
27. For requests involving children aged 12 and over, the Information Management Team will contact the parent to advise that the child's consent is required before the request can be progressed

unless they feel that their child does not have the required capacity. The parent shall also be informed that the information will be provided to the child, and it will be the child's decision to share the information with the parent. If the parent or guardian advises that the child does not have the necessary capacity to understand due to, for example learning difficulties, the above procedure should be followed with the information being provided to the parent or guardian.

Subject Access Request Process



Other Data Protection Rights

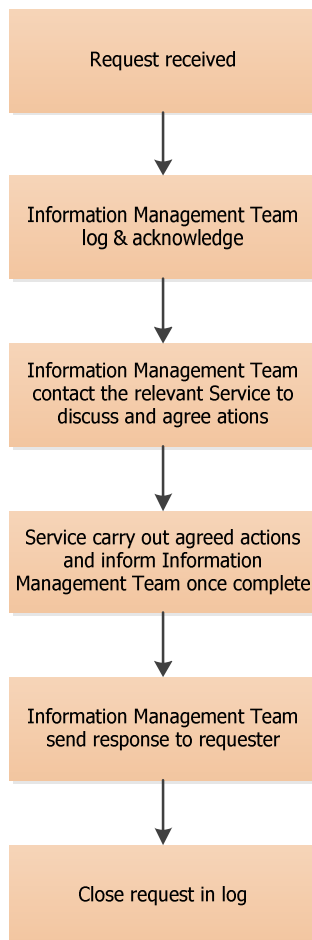
Individuals are afforded other rights than just access and these are:

- Right to object to the processing of their personal data
- Right to request inaccurate data to be rectified
- Right to request that the processing of their personal data is restricted.
- Right to request that their personal data is erased.
- Right to request a copy of their personal data in a structured, commonly used, and machine-readable format (Data Portability)

These rights are subject to the legal basis for which the processing is relying on and therefore may not apply. However, the Council must give full consideration to each request whether or not it applies in each case and must do so within 30 calendar days.

A full explanation must be provided to the individual making the request whether the Council is complying or refusing the request and why.

Any request should be forwarded to the Information Management Team as soon as it is received. The request will be validated, logged, and acknowledged. The Information Management will then discuss with the service involved. Once discussed the Information Management Team will send a response to the individual and close the request in the log.



Appendix 1 - SAR Distribution Template

A valid Subject Access Request under Data Protection legislation has come into the council that needs to be responded to. It is important that this request is considered by all relevant members or staff / services in order to ensure a comprehensive search is undertaken.

This request **must be** responded to within 30 calendar days. Your response should be sent for approval no later than 15 calendar days.

If you need additional support with handling this subject access request, please contact [insert name of Information Officer] who is dealing with this request.

Your response must be securely shared with your coordinator to arrange for approval no later than [insert date]. It is important that you include a response below for inclusion in the Council's letter and complete the search template. If this information is not provided the coordinator will ask for this to be completed.

Date Validated	
Name of third party	
Name of third-party organisation	
Name of data subject	
Data subject DOB	
Address or other identifiable	
Information requested	
To: Department(s)	

The following must be completed by staff handling subject access request.

Response to the data subject: The Council has a duty to provide advice and assistance. At a minimum, your response should include the rationale of any redactions carried out (i.e., third party personal data) and whether any information has been withheld in full, and why.	
--	--

SAR Request – Information Searches		
ONE FORM TO BE COMPLETED PER PERSON		
	Tick area searched	Tick where information sourced
Emails (including generic mailboxes)		
Shared Drives / One Drive		
SharePoint sites		
Corporate Business Applications e.g., Jadu, Mosaic, SEEMiS, Uniform, Business World, Lexi, She Assure etc.		
Other electronic applications e.g., MOMO, Showbie etc.		

Paper documentation e.g., handwritten notes		
Iron Mountain		
Other electronic equipment e.g., mobile phones, iPad, CCTV etc.		
Other (please specify)		
Your name		
Your job title		
Your department		

Subject Access Request Form

When making a Subject Access Request you must:

- supply information to prove who you are (to eliminate risk of unauthorised disclosure); and
- provide as much detail as possible regarding the information you wish to access (e.g., where and by whom information is believed to be held, specific details of information required).

You are not required to state WHY you wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.

You must provide one proof of identity document (e.g., current full or provisional driving licence, passport, birth certificate). Additional information may be required in order to validate your request.

Your Personal Details *(please print clearly in black pen)*

Surname: _____ Date of Birth: _____

First Names: _____

Email address: _____

Address: _____

_____ Post Code: _____

Phone (day): _____ Phone (eve): _____

The data you wish to access

Please give us details of all the personal data you would like to access in the box provided below.

If you are looking for information about a particular period of time or circumstances in which you dealt with Social Work Services, please state the dates or circumstances you are interested in.

We ask that you be as specific as possible.

Please provide details of any reference numbers or information relating to family members that may assist us to locate the information you require.

Please tick the appropriate box below

☐ Homelessness

☐ Council Tax

☐ Welfare Benefits

☐ Building Control

☐ Social Services

☐ Safer Communities

☐ Education

☐ Regulatory/Licensing

☐ Human Resources

☐ Planning

If you are seeking access to your child’s educational record, and you have parental rights and responsibilities, please contact the school directly as this is not a subject access request. Schools are regulated by the Pupils’ Educational Records (Scotland) Regulations 2003. Schools have 15 school days to handle valid requests.

Additional Information

Declaration

I request that you provide me with a copy of my personal data that you process for the purposes I have indicated above.

I confirm that I am the individual the information may relate to and not someone acting on their behalf:

Signed: _____ Date: _____

Third party (to be completed by person(s) acting on behalf of the data subject)

I confirm that I am acting on behalf of the individual the information may relate to and attach letter of authorisation and necessary identification.

Signed: _____ Date: _____

This form should be returned in person to any Council Contact Centre or by post to the Information Management Team, Scottish Borders Council, Headquarters, Newtown St Boswells TD6 0SA.

ID Verification (for internal purposes - to be completed by Information Management Team)

Identity Check – Data Subject/Third Party must produce one of the following before they are allowed access to the information.

Birth Certificate: ☐

Passport: ☐

Driving Licence: ☐

Utility Bill: ☐

Third party: Letter of authorisation/identification: ☐

Checked by: _____ (Print name)

Appendix 3 - Information Sheet for the Public

How to Access Information about You

Data Protection provides you with the right to request confirmation if we are holding and using your personal data, what personal data we are using, who we share it with, how long we will keep the data for and what your rights are over how it is used. You are also entitled to ask for a copy of your personal data that we hold, and this is called a Subject Access Request.

We wish to provide a prompt response to your request for access to your personal data. You should provide as much information as possible when making such a request to help identify the information you are seeking. We may need to verify your identity and ask for a copy of ID such as a passport; driving licence or birth certificate along with a bill with your current address dated within the last three months.

You are entitled to a response within thirty calendar days. However, if the information being requested is both large in volume and complex in nature the Council can apply an extension of up to three months. You will be informed as quickly as possible if this is deemed necessary.

You are only entitled to your own personal information. You may only ask for information about another person if you have appropriate authorisation to act on their own behalf i.e., a signed letter of consent or it is deemed reasonable that the person is not able to give their consent and appropriate measures have been taken to try to obtain consent.

If you are wishing to request information regarding a child over the age of 12, please be advised that the child's consent will be required and any information held will be provided to the child who can then choose to share it with you. This is because Scots Law states that a child over 12 years of age has the capacity to understand unless otherwise proven and it is the child who is entitled to access their personal data.

You can make your request by email to dataprotection@scotborders.gov.uk ; on our website using our [online contact form](#) or by completing our form which you can either email, hand into one of our contact centres or by post to:

The Information Management Team
Legal & Licensing
Regulatory Services
Scottish Borders Council
Headquarters
Newtown St Boswells
TD6 0SA

Please note that any information you provide in relation to your request and the result of the search will be held on computer for the purpose of managing your request and this will be retained for three years. This information will be passed to relevant employees of the Council in order to comply with your request. If your request involves information provided by other organisations such as the Police, NHS, other Local Authorities, the organisation may also be made aware of the request.

The Data Protection Officer for Scottish Borders Council is Nuala McKinlay, who can be contacted by phone 0300 100 1800; email dataprotection@scotborders.gov.uk or by letter at the address provided above.

The Regulator for data protection is the UK Information Commissioner (ICO): Online:
<https://ico.org.uk/make-a-complaint/>

By telephone: 0303 123 1115
By email: Scotland@ico.org.uk

By post:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF