Barth Syndrome UK Subject Access Request Policy

Reviewed: **02.12.2019 / 02.12.2020 / 02.12.2021 / 19.04.2023**

Next Review Date: 19.04.2024

1 Introduction and purpose

The Data Protection Act 2018 (the Act) gives individuals rights of access to their personal records held by Barth Syndrome UK (BS UK). Subject access is a fundamental right for individuals. But it is also an opportunity for our organisation to provide excellent customer service by responding to Subject Access Requests (SARs) efficiently and transparently and by maximising the quality of the personal information we hold. This Policy explains how the organisation will fulfil its obligations under the Act.

2 Policy Statement

The organisation regards the Act as an important mechanism in achieving an honest, safe and open relationship with its members and supporters.

Subject access is most often used by individuals who want to see a copy of the information the organisation holds about them. However, subject access goes further than this and an individual is entitled to be:-

- Told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the personal data.
- Given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision for benefit or a grant entitlement, or an assessment of performance at work.

The aim of this policy is to ensure that Barth Syndrome UK complies with its legal obligations under the Data Protection Act 2018 and can evidence that it has done so. It also aims to ensure that the charity:-

- Has robust processes in place for dealing with SARs, saving time and effort.
- Increases levels of trust and confidence by being open with individuals about the personal information we hold.
- Improves the transparency of our activities in line with public policy requirements.

3 Scope of the Policy

This document outlines how an applicant can make a request for their personal information under the Act and how it will be processed.

This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information.

This document takes into account the key features of the Act and outlines how the organisation will take steps to ensure compliance in relation to requests for personal information.

Requests for access to the records of people who are deceased are not within scope of this Policy as the Act only applies to the data of living individuals. Such requests will be treated as requests for access to information under the Freedom of Information Act or as miscellaneous requests, depending on the nature of the data and the reason the data is being requested.

4 Key Definitions

Subject Access Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of Information Request or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relates to a living individual who can be identified directly or indirectly from the data. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
Special Category Data	Certain personal data, special category data, is given special protection under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Special category data includes: - • a person's racial or ethnic origin. • political opinions. • religious or similar beliefs. • trade union membership. • physical or mental health or condition or sexual life.

	• biometric or genetic data.
Data Controller	The organisation which determines the purposes, and the manner in which, any personal data is processed is known as the data controller. The organisation is the data controller of all personal data used and held within each part of the organisation
Data Processors	Organisations or individuals who process personal data on behalf of a data controller are known as data processors. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Third Party	An individual who is not the subject of the data but may be connected to or affected by it is known as a third party.
Relevant Professional	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.

5 Duties of the Information Commissioner's Office

The Information Commissioner's Office is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, ruling on complaints and taking appropriate action when the law is broken.

The Information Commissioner's Office is responsible for ensuring compliance with the Act and Data Protection in practice for all organisations in England, Scotland, Northern Ireland and Wales.

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audits. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller for breaches of the Act.

If organisations are found to be in breach of the Act the Information Commissioner's Office may issue undertakings committing an organisation to a particular course of action in order to improve its compliance.

The Information Commissioner's Office can serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.

The Information Commissioners Office conduct consensual assessments (audits) to check organisations are complying. In cases of serious breaches the Information Commissioner's Office may issue a monetary penalty notice, requiring organisations to pay a fine of up to €20 million.

The Information Commissioner's Office can prosecute those who commit criminal offences under the Act. This includes organisations and individuals.

6 Roles and Responsibilities

Adhering to the Data Protection Act 2018 is the responsibility of every trustee and member of staff acting for or on behalf of the organisation. Subject Access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information is considered to be part of every trustee and staff member's role.

Your primary responsibility is to ensure that Subject Access Requests are in the first instance directed to the Chief Executive or the Chair. They will log the request, acknowledge it and may pass the case to a designated person within the organisation for response. It is important that requests are processed as soon as they are received to assist in meeting the statutory deadline.

Board of Trustees	The Board of Trustees holds overall responsibility for compliance with the Act.
Chief Executive	The Chief Executive (or Chair where there is no Chief Executive) has responsibility for the management of Subject Access Requests; this includes dealing with complaints from the Information Commissioners Office, general compliance issues and data subject queries and concerns. Ensures that SARs are responded to in a timely manner and that only data that the data subject is entitled to access are sent out. Also responsible for completing a double check of all SAR's before they are securely dispatched.
Employees	All employees, including temporary staff, must understand their duty of care to ensure the confidentiality of all personal data. In addition, they must have an understanding of this policy and where to direct individuals enquiring about subject access requests.

7 How can an individual make a SAR?

A valid SAR must always be made in writing, either via email or post.

It is quite common that a request for personal data can be linked with a complaint, or a Freedom of Information request.

NOTE: No matter how a request is received there is no requirement for the requester to mention either the Data Protection Act or Subject Access for it to be a valid request. In some cases, the requester may even state the wrong legislation e.g., Freedom of Information Act, but the request will still be valid.

Either way, it is the responsibility of the person dealing with the request to appropriately recognise a request as one for personal data, i.e., information relating to the requester, and process it accordingly. Failing to recognise a SAR is not an excuse for non-response and the organisation will still fall foul of the Data Protection Act should a response not be provided in a prompt and appropriate manner.

8 Can individuals request personal information on behalf of another person?

Yes, they can. The Act allows for an individual to make a request on behalf of another person. This may be a solicitor acting on behalf of the individual, a parent making a request for their child's information, a third party making the request for someone who has limited capacity, or indeed many other reasons. However, whilst the Act allows us in certain circumstances to process a request in this way, there are a number of considerations and checks that need to be undertaken before you process a request which is made on behalf of another person. For example, a parent is not necessarily automatically entitled to information about their children.

9 How long do we have to respond?

The organisation has a maximum of a month starting from the day the request and identification (if required) is received. This is a statutory requirement which must be adhered to. In exceptional circumstances an extension can be agreed.

10 Can I charge for the request?

No - you must provide a copy of the information free of charge.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

11 What do I do if I receive a request?

In practice, if someone wants to see a small part of their data you need to apply common sense. You should not require a formal SAR if the individual can prove their identity, the information is readily available there and then, and no other third-party data will be unreasonably released. Such requests should be dealt with quickly, as business as usual and with little formality.

All other ("non-routine") requests for personal data which are likely to take a reasonable amount of resource must be directed to the Chief Executive or Chair and be logged.

12 How do I locate the information requested?

Processing a subject access request can prove very difficult if you do not have adequate information systems in place. Well-structured file plans and standard file naming conventions within organisations should be in place to assist in locating information easily.

Poor file management / knowledge of systems cannot be used as a reason for being unable to respond to a SAR effectively.

Requests for information are not limited to “live” files. SARs cover all information held by the organisation regardless of the format it is in or where it is stored, closed, archived, and in some cases even deleted information (e.g., located in outlook deleted items) should be considered as part of a request.

Unfortunately, there is no outright exemption or time threshold with regards to the amount of time it may take members of staff to locate SAR information.

13 Can I provide all information found relating to the data subject?

The simple answer is no.

The organisation must consider whether it is possible to comply with the SAR without revealing information that relates to and identifies a third-party individual or any other exempt information.

Examples of third-party information that cannot be shared routinely without specialist consideration are: -

- Safeguarding concerns which may contain information about multiple children including siblings and estranged parents.
- Files containing legally privileged information.
- Files containing advice from relevant professionals such as doctors, police or probation services.
- Employee files containing information identifying managers or colleagues who have contributed to (or are discussed in) that file.

Special consideration should be given to sharing this type of information.

14 What is a double check?

Before a SAR is sent out to the data subject another trustee of the Charity is required to carry out a double check. This is done to ensure that all third-party data has been removed appropriately and that any documents have been redacted appropriately.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the organisation (see section 5 above).

The Board of Trustees are responsible for completing a double check of the information to be provided to the data subject.

15 How do I respond to a SAR?

Once all the information has been collated (duplicates and third-party information has been removed or redacted and a double check has been carried out) the information will be provided either in paper copy, electronically or during a meeting with the Data Subject and sent securely.

The organisation is required to provide the copies in a format requested by the data subject.

16 Complaints

The organisation will provide a right of complaint to all applicants in the event they are dissatisfied with the handling of their request. If an applicant is unhappy with the service they have received, they should firstly contact the Chief Executive or Chairperson.

If the applicant is dissatisfied with the content of the information they have received, they should also make a complaint in writing to the Chief Executive or Chairperson. If an applicant remains dissatisfied with the outcome of their Stage 1 complaint, the Chief Executive or Chairperson may seek legal advice and may ask the Information Commissioner's Office to carry out an independent investigation.

16.1 Appealing a decision to refuse disclosure of Information

If the organisation refuses to disclose information in response to a subject access request, the organisation should offer the applicant an opportunity to appeal the initial decision. If the applicant believes that an error has been made in the response to their SAR, they are able to appeal the organisation's decision by seeking an internal review with the Chairperson.

Once an appeal has been received, the complainant will receive an acknowledgment receipt and the request and response to it will be reconsidered.

The applicant will be notified of the outcomes of the internal review as soon as possible. All internal reviews should be concluded within 20 working days.

If an applicant's appeal is successful, they will receive the information they requested as soon as possible. If the appeal is unsuccessful the organisation will provide a detailed explanation of the findings and supply further information on how to take the matter further.

16.2 Complaining to the Information Commissioners Office

If an applicant is not satisfied with the outcomes of the organisation's decisions, they have the right to submit a complaint to the Information Commissioner's Office. The Information Commissioner's Office will make an initial assessment of the case before carrying out an investigation.

The Information Commissioner's Office has written guidance notes for applicants on how to complain to the Information Commissioner's Office and published it on their website www.ico.gov.uk

17 Related documents

- Data Breach Policy
- Data Protection Policy

- Document Retention Policy
- Information Security Policy