Policy No. 901
Template Ver: April 2023

Data Protection Rights Request Policy and Procedure	
Originated by:	David Traynier, Head of Quality and Compliance & Data Protection Officer
Date Ratified:	13/10/2021
Ratified by:	Title of Group or Person
Revised by: N/A Revision No. 000 Ratified by: N/A Date ratified: N/A	Date: N/A
Date of next review: 01/10/2024	
Document Owner:	Data Protection Officer
Document Classification:	Internal

Revision Summary

- 10/2021 This is a new policy.
- NB this policy supersedes St Helena's Patient Access to Hospice Health Records Policy and Procedure [098].

Revision History

- N/A

Policy Statement

What is this policy intended to achieve?

The (UK)GDPR and the Data Protection Act 2018 (DPA) provide individuals with eight rights over the personal data we hold about them. This policy and procedure defines the process you should follow if you are involved in a request to exercise one or other of these rights. Failure to comply properly with a Data Protection Rights Request (DPRR) may leave St Helena liable to administrative fines from the Information Commissioner's Office (ICO).

To whom does this policy apply?

This policy applies to all members of staff and volunteers.

Who should read this policy?

All Directors, departmental managers, and clinical team leads should familiarise themselves with this policy. Managers should also ensure that their teams are trained to recognise DPRRs when they receive them. Non-clinical heads of department should ensure they have designated lead for dealing with DPRRs and liaising with the Data Protection Officer.

Definitions and Terminology

Data protection rights request. This is the ICO's term for any request an individual makes to exercise their lawful data rights.

Rights of the Data Subject

Under the (UK)GDPR Articles 12-23, anyone whose personal data we process has rights with respect to that data. These rights are:

- The right to be informed.
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights relating to automated individual decision-making, including profiling

These rights are subject to various exemptions and are also conditional upon the lawful basis under which the information is processed. For a more detailed discussion of each of these individual rights, please see Appendix One – Subject Rights in Detail. For further clarification, consult the Data Protection Officer.

What is a valid Data Protection Rights Request?

A Data Protection Rights Request (DPRR) is any request, made by a person to exercise one or more of their eight data subject rights. The applicant does not have to phrase their request in any particular way, use any particular form or refer to the relevant legislation. All the applicant needs do to trigger the process is make it clear that they want to exercise one of their lawful rights. Requests can also be made by third parties authorised by the data subject. For a request to be valid and actionable, it must meet two criteria:

- It provides all the information we require to locate the information concerned; and
- It provides sufficient information for us to verify the applicant's identity.

Distinguishing DPRRs from normal requests

St Helena processes information about patients, employees, family members, and others in the normal run of its business. During that business we may provide someone with a copy of information we hold about them or correct or update their data. It is important to distinguish such normal requests from formal DPRRs and respond appropriately. Where necessary, managers should clarify with applicants whether they are looking to exercise their full rights under the (UK)GDPR. If a request is a simple one as part of normal business, which can be responded to promptly and simply, it should be treated as such. The DPRR process is more likely to be appropriate where an individual requests a high volume of information that will require a time-consuming search, for us to stop processing their data or for us to delete it.

Fees

We cannot charge a fee to comply with a DPRR, unless either of the following conditions applies:

- The request is 'manifestly unfounded or excessive.' In cases where a manager feels that a request is unfounded or excessive, they should consult with the DPO who will advise on whether the ICO's definitions of these terms is satisfied.

- We may also charge a fee if an applicant requests further copies of their data following their initial request.

If either condition is satisfied, a ‘reasonable fee’ for administration costs may be levied. This may include the costs of assessing whether we have the information, locating and retrieving it, communicating with the person requesting it, and providing them with a copy or a response where we do not provide the information. Where the request is judged to be unfounded or excessive, the rationale for this decision should be communicated to the applicant, along with a cost breakdown explaining the fee to be charged.

Timeframes

We are required by law to respond without undue delay and, at the latest, within one month of receipt. The clock begins the calendar day after the request is received. Note that this does not mean the first day that a member of staff becomes aware of the request but the day the email or letter is received, so managers should keep this in mind. So, if the request is received on Monday 4th March, the clock will start on Tuesday 5th of March and the deadline will be 4th of April. If this is not possible because the month is shorter, then the deadline is the last day of the following month. Where the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

Note. Upon receipt of a request, we are required to verify the applicant’s identity. It is permissible here to stop the clock until the applicant has provided the required information.

Note. Where the application is a subject access request and it is reasonable to ask the applicant to clarify the information they are seeking, the clock can be stopped until they respond. Where we seek clarification, but do not receive a response, we should wait for a reasonable period before considering the request ‘closed’. One month is generally reasonable, but this may be extended if there are reasonable grounds to do so, such as the applicant having genuine difficulties. We have a legal duty to make ‘reasonable

adjustments' for anyone who is disabled, and efforts should always be made to accommodate applicants as much as is practicable.

If we also need to clarify a DPRR, we should not wait until the applicant provides this before then asking for ID documents, unless any clarification risks disclosing personal data to the individual before we have checked their identity.

Extending the deadline.

It is permissible to extend the response time by a further two months to a maximum of three calendar months. We can do this for two reasons only:

- The request is complex.
- The applicant has made several separate requests, at the same time, of that department.

In cases where a manager thinks an extension is justified, they should first consult with the Data Protection Officer. Following this, they must contact the applicant within one month of receiving their request and inform them of the reasons for the extension and the justification for it. It is best practice that we notify the applicant of this extension as soon as possible and not use it as a fallback as the one month deadline approaches. Extensions may not be used merely because of pressure of work.

Event	Clock Status
Request received	Clock starts
Request for identification sent	Clock stops
Request for clarification of data sought (access requests only)	Clock stops
All requests met	Clock starts
Initial deadline	One calendar month from most recent clock start
Extended deadline	Three calendar months from most recent clock start

Breaches

Where the DPRR module detects a deadline is approaching, it will notify the Data Protection Officer and the relevant manager automatically.

Breaches of timeframe must be logged on Sentinel and will be reported to the Senior Management Team as part of the quarterly Information Governance Report. For the purposes of this, the following will count as a breach:

- Failing to comply within one month when no extension was requested.
- Failing to comply with an extended deadline.
- Failing to comply within three calendar months.
- Failure to comply.

Complaints

Where an applicant is not happy with our response to a DPRR, this should be treated as a complaint and logged accordingly. In these cases, we should offer a review of the case by the DPO who will then communicate the result of this to the applicant. Where the applicant remains unsatisfied, we should assist them in making a complaint to the Information Commissioner's Office. In such cases, St Helena will cooperate with any ensuing investigation and comply fully with any findings.

The process

The following description of process is written with a view to subject access requests because this is by far the most common type of request. The process for handling other DPRRs follows broadly the same pattern with only minor variation.

1. Receipt and initial assessment
2. Identity verification
3. Data assessment
4. Actioning
5. Response
6. Archiving

1. Receipt and initial assessment

A DPRR does not have to meet any formal requirements to be a valid request. An applicant can make a request verbally or in writing, including via social media. They can make it to any part of St Helena, and they do not have to direct it to a specific person or contact point or mention any legislation. Applicants do not have to give reasons for their request or state what they intend to do with the information.

All staff and public/patient facing volunteers should be able to take the details of a request and log it on the Sentinel DPRR module, as they would a complaint. Care should be taken to establish the precise nature of the request. Where there is doubt, advice should be sought from the DPO without delay. DPRRs should also be distinguished from complaints, but there may be circumstances in which the request is part of a complaint. If so, the complaint must always be logged separately on the Complaints module and then cross-linked to the DPRR.

Departments receiving DPRRs must log them on the Sentinel DPRR module within 24hrs of receipt. This will notify the Quality & Compliance Department and the DPO will advise on the lawfulness of the application, any exemptions that might apply, and the forthcoming process.

2. Identity verification

Individual managers should take a common-sense and proportionate approach to verifying an applicant's identity (including their current address). If the applicant is known to them, they are in an active professional relationship (e.g. an active supporter, donor or patient) with them or a previously established correspondence, and the data requested is not especially sensitive, then it should not be necessary to confirm their identity. In this circumstance, a manager within the receiving department may vouch for the identity of the applicant. This vouching should be documented. Requesting identity documents should not be a default.

Where there is doubt about the identity of the applicant, however, it is important that the manager responding to the DPRR takes necessary steps to document that the

applicant's identity is confirmed. As per the third data protection principle, staff should ask only for the minimum additional information required to verify identity. Copies or photographs of the following forms of identification may be accepted. Two items should be required of which one should provide photographic ID.

- Current UK/EEA Passport.
- UK Driving Licence.
- Financial Statement issued by bank, building society or credit card company.
- Utility bill for supply of gas, electric, water or telephone landline/internet connection.
- Mobile telephone contract account.
- Firearm Certificate
- DBS Enhanced Disclosure Certificate.
- Birth Certificate
- Buildings, contents, or vehicle insurance.

Note: where the request is for medical records and is coming from a solicitor or insurance company, the originating company and email address should be verified. Where necessary, a phone enquiry may be made to the company, to confirm the request.

Requests from the police or law enforcement agencies should be confirmed with appropriate identification from the officer making the request, such as a warrant card. If contact is made over the phone and there is any doubt, their name, badge number, and station should be requested for a return call.

Other requests made by a third party on behalf of a data subject should be verified and steps taken to communicate with the data subject or otherwise establish that the request is authorised. Where there is doubt, the relevant manager should consult with the DPO.

3. Assessment and evaluation

At this point, the responsible department (consulting with the DPO) should assess the validity of the request. We will need to establish that we hold relevant data and whether the lawful basis under which we process the data allows for the action requested. It is at this point where any other, competing obligations should be considered, such as legal requirements or duties to other data subjects. There may also be applicable lawful exceptions.

The receiving Department and the DPO should assess the scope of the data involved in the request. Specifically, to which departments and systems the request applies. For instance, if a Lottery player requests that their data is erased from Lottery systems, it should be confirmed that the erasure (and therefore the preceding search) will not apply to data held by Fundraising. However, a request from an employee to see all information held about them by St Helena would have to encompass the whole organisation.

Back-up and recovery data

DPRRs also apply to our backup systems, so they should be searched or amended as necessary. This is particularly pertinent to requests for erasure. Where there is a rolling back-up and data will be overwritten according to an established schedule, it is acceptable to allow this process to occur as normal. In cases where back-ups are not automatically overwritten or deleted, then efforts should be made to remove or edit them manually.

In cases where data cannot be immediately overwritten, it will be sufficient that it is 'put beyond use.' This is defined as follows:

- We are not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- We do not give any other organisation access to the personal data;

- We ensure the data is still protected with appropriate technical and organisational security measures;
- We commit to, and schedule, permanent deletion if, or when, this becomes possible.

All instances where deletion is not possible will be logged on the Sentinel module along with an appropriate action plan and review date. These will be monitored by the Quality & Compliance Department. Where erasure of back-ups is not possible, this situation must be explained to the applicant, and this documented on the module.

4 Actioning

It is at this stage that we will fulfil the request. Where the DPRR concerns data processed by a single department, it is the responsibility of that department to action it. Where the request encompasses processing by more than one department or the whole organization, the Quality & Compliance Department will coordinate a response from the appropriate departments.

All departments receiving a request for assistance from the Quality & Compliance Department are required to acknowledge receipt of the request in two working days and to respond within one working week. Each department is required to action the request in respect of its own electronic and paper databases, all of which should be registered on the Sentinel Information Asset Register. The IT department will assist as necessary.

Where it is required to search files and folders on St Helena's SharePoint tenancy, the IT Department will do this, with direction and support from the Quality & Compliance Department. These searches will cover all data stored in Office365 email accounts, shared or personal OneDrives, Teams, and SharePoint.

All DPRRs include any paper records held in structured filing systems. The (UK)GDPR defines a filing system as 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.'

A filing system is structured if it passes the ‘temp test’; i.e. that a new, temporary member of administrative staff could successfully retrieve a specific piece of information within a short time.

Note. Under the Data Protection Act 2018, personal data held in unstructured manual records processed by public authorities is included under the right of access. This includes paper records that are not held as part of a filing system. Therefore, all Patient and Family Service records relating to service users must be included in subject access requests, whether electronic, structured paper records or unstructured paper records.

Patient Access to Records Requests

Requests for patient records that are not part of a formal subject access request should be referred in the first instance to the Caldicott Guardian for approval. These requests will be processed by the PA to the Director of Care and will cover both SystmOne modules, call logs, and any other records maintained by St Helena staff. Emails will not normally be included, although this can be decided case-by-case. If the applicant, who will most commonly be a relative rather than a patient, makes clear that they want to see all information held about them, this should be treated as a subject access request. All retrieved records will be reviewed by the Caldicott Guardian prior to release.

Records may be shared in hard copy or electronically, as appropriate. If made available in hardcopy, they may only be presented to the applicant in person or delivered by recorded mail. Electronic records should be shared using a confidential Microsoft Teams channel via a hyperlink. For more advice on this, consult the Data Protection Officer or the Head of IT.

When providing records to the applicant, the Caldicott Guardian will decide whether a face to face meeting should be offered to assist the applicant in interpreting the notes.

Records can also be provided to authorised third parties, including solicitors, insurance companies, and law enforcement agencies. In this instance, it will not be necessary to offer a face to face meeting. Staff dealing with these requests should require evidence

that requests made by third parties are authorised and should take steps to contact the data subject directly where there is doubt.

All patient access to records requests must be logged on the Sentinel DPRR module.

5. Response

Reponses to DPRRs should state clearly what has been done to action them, e.g. which data has been erased from where, which recipients or other controllers have been contacted, how data has been rectified, and so forth.

Where we are responding to a subject access request, we should provide the requested information in a manner that is concise, transparent, intelligible and in easily accessible form, using clear and plain language. Commonly, data can be supplied in .csv file format, but the IT department can advise on this.

Note: It is important to note that for SARs, our obligation is to provide information and not simply documentation. There may be occasions when it is appropriate and convenient to the applicant for us to provide copies of individual documents, emails, etc. Much of the time, however, it will be enough that we provide a summary of the information held in documents.

When responding to DPRRs, the following supplemental information should also be included:

- Our purposes for processing the data;
- The categories of personal data we are processing;
- Any recipients (or categories of recipient) to whom we have or will be disclosing the personal data;
- The retention period or, if there isn't one, the criteria for determining how long we will store it;
- The applicant's right to request rectification, erasure or restriction or to object to processing;
- The applicant's right to lodge a complaint with the Information Commissioner's Office (ICO);

- If the data wasn't obtained directly from the applicant, details of its origin;
- Whether or not we use automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual;
- The safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

Secure sharing

When responding to a subject access request, any information must be supplied to the applicant securely and in electronic form unless the applicant requests otherwise. The information should be made available to the applicant using a confidential Microsoft Teams channel via a hyperlink. For more advice on this, consult the Data Protection Officer or the Head of IT. If made available in hardcopy, the information may only be presented to the applicant in person or delivered by recorded mail.

6. Archiving

All DPRRs will be retained on Sentinel for a period of six years unless a valid exception is proposed. After six years, they will be flagged for deletion.

Associated Policies and Procedures

- Information Governance Policy [900]

Compliance with Statutory Requirements

- Data Protection Act 2018

Responsibilities/Accountabilities

Title	Accountability
Chief Executive Officer	Overall responsibility for compliance with this policy.

Title	Accountability
Data Protection Officer	First line responsibility for ensuring compliance with this policy.
Caldicott Guardian	Responsible for ensuring we have a compliant system for providing access to patient records.
Directors and service managers	Responsible for ensuring that their accountable areas comply with this policy and cooperate with the Quality & Compliance Department.

Staff Training Requirements

Directors and service managers should ensure they have a link member of staff familiar with this policy and able to support the Quality & Compliance Department.

Monitoring (Including Audit) and Frequency of Review

This policy will be reviewed every three years. The Quality & Compliance Department will monitor compliance with DPRR standards.

Data Protection

Does this Policy require sign off from the Data Protection Officer?	Yes
DPO approved: David Traynier	Date: 25/10/2021
DPO comments	Policy written by DPO.

References:

1. Data Protection Act (2018)
2. Information Commissioner's Office 'Guide to the General Data Protection Regulation (GDPR)', March 2021 edition, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf
3. Information Commissioner's Office (2020) 'Right of Access,' available at https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf

Equality Impact Assessment Initial Screening Tool

Document Reviewer(s):	David Traynier, Head of Quality & Compliance	Date Assessment Completed:	25/10/2021

Assessment of possible adverse impact against any minority group			
Could the document have a significant negative impact on equality in relation to each area below?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Age		X	
2. Sex		X	
3. Disability		X	
4. Race or Ethnicity?		X	
5. Religion and Belief?		X	
6. Sexual Orientation?		X	
7. Pregnancy and Maternity?		X	
8. Gender Reassignment?		X	
9. Marriage and Civil Partnership?		X	

- You need to ask yourself:
- Will the document create any problems or barriers to any community or group?
- Will any group be excluded because of this document?
- If the answer to either of these questions is yes, you must complete a full Equality Impact Assessment.

Assessment of positive impact			
Could the document have a significant positive impact by reducing inequalities that already exist?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Promote equal opportunities		X	

2. Eliminate discrimination		X	
3. Eliminate harassment		X	
4. Promote positive attitudes towards disabled people		X	
5. Encourage participation by disabled people		X	
6. Consider more favourable treatment of disabled people		X	
7. Promote and protect human rights	X		This policy will help us better service people's data subject rights.

On the basis of the information/evidence/consideration so far, do you believe that the document will have a positive or negative adverse impact on equality?

Positive	Please rate (delete as applicable) the level of impact					Negative
		LOW				

Is a full equality impact assessment required? No

Appendix 1 – Subject Rights in Detail

The following section provides a more detail description of each of the rights available to UK data subjects under the UK(GDPR) and the Data Protection Act 2018.

The right to be informed

The right to be informed concerns St Helena's obligation to provide 'fair processing information' to people about how we process their data.

The principal means of us doing this is through the Transparency Notice on our website, which should explain how we handle personal data across our services. Where required or reasonable, each service will also provide such information at the point personal data is collected. The information we supply must be;

- Concise, transparent, intelligible, and easily accessible
- Written in clear and plain language
- Freely available

The information that we must supply is determined by whether we obtain directly from the data subject. This also determines when we should provide the information.

When we obtain data directly from the data subject, we should provide the information at the time we collect it.

When we collect the data indirectly, we should provide information to people as soon as possible and within one month.

- If the data are used to communicate with the data subject, at the latest, privacy information should be provided when the first communication takes place; or
- If disclosure to another recipient is envisaged, at the latest, it should be provided before the data are disclosed.

The table below is a guide to what information should be supplied.

Information to be supplied	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	YES	YES
Purpose of the processing and the lawful basis for the processing	YES	YES
The legitimate interests of the controller or third party, where applicable	YES	YES
Categories of personal data	NO	YES
Any recipient or categories of recipients of the personal data	YES	YES
Details of transfers to third country and safeguards	YES	YES
Retention period or criteria used to determine the retention period	YES	YES
The existence of each of data subject's rights	YES	YES
The right to withdraw consent at any time, where relevant	YES	YES

The right to lodge a complaint with a supervisory authority	YES	YES
The source the personal data originates from and whether it came from publicly accessible sources	NO	YES
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	YES	NO
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	YES	YES

The right of access

Data subjects have the right to access the data we hold about them (and supplementary information) to be aware of and verify the lawfulness of our processing. They have the right to:

- Receive confirmation that we are processing their data
- Access their personal data
- Other supplementary information (the information that should already be provided in the Transparency Notice)

This information must be provided free of charge; however, we may charge a reasonable administrative fee for requests we deem to be manifestly unfounded or excessive (e.g. repetitive). In such cases, we may also decide not to comply with the request. In all cases where we choose not to comply with a request, we must, within one month, give the applicant a full explanation of our reasoning. We should also inform

them of their right to complain to the Information Commissioner's Office and to take legal action.

We can charge a fee for additional copies of the same information, although not for further separate requests. These fees must not exceed the administrative costs we incur. Where we hold a large amount of data about a subject, we may ask them for the specific information they require. We will not retain personal data for the sole purpose of being able to react to potential requests.

The right to rectification

Individuals have the right under Article 5(d) to expect that the data we hold about them will be 'accurate and, where necessary, kept up to date'. To this end, we have a duty to correct a data subject's information whenever it is inaccurate or incomplete.

In any instances where we have disclosed the information to third parties, we will take reasonable steps to provide those parties with the corrected information. As appropriate, the data subject should also be given the details of all third parties with whom we have shared the incorrect information.

The right to erasure

The right to erasure is sometimes known as the 'right to be forgotten' and allows data subjects to have the data we hold about them erased or destroyed where there is no compelling reason for us to hold it or process it any longer. They do not have to demonstrate that the processing has or will cause them any harm or distress, although if it does this would make their claim more compelling. The right to erasure is not absolute and applies only in the following circumstances:

- 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 (i.e. otherwise in breach of the (UK)GDPR)
- The personal data must be erased to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Decisions about whether to comply with a request should consider the lawful basis under which the data was initially collected. This should be documented in the Record of Processing Activities (ROPA).

There are specific limitations to this right and a request can be refused in if the data is being processed for any 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 or historical research, or statistical purposes
- If St Helena needs the information for the exercise or defence of a legal claim.

Where the data has been shared with other organisations, reasonable efforts should be made to inform them of the request. In cases where we have made the data public, we will take reasonable steps to inform any other organisations who are processing the data so that they can erase any links to, or copies or replications of the data.

Special requirements relating to children's data

Special consideration should be given where the data subject gave their consent as a child and was not fully aware of the risks involved by the processing and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

The right to restrict processing

Data subjects have a limited right to request that we restrict processing of their data. In this context, 'restriction' means that the data can still be held but it cannot be used or processed in any other way. We are required to restrict processing in the following circumstances:

- Where the person disputes the data, processing should be restricted the processing until the accuracy of the data has been verified
- If the person has objected to the processing (see Page 7) and the lawful basis is either 6(1)(e) 'necessary for the performance of a public interest task' or 6(1)(f) 'legitimate interests' and that request is still being considered
- When processing is unlawful, and the individual opposes erasure and requests restriction instead
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Appropriate methods of restriction may include temporarily transferring the data to another processing system, making it unavailable to users, or temporarily removing it from a website. When data is restricted on an electronic system, it should be flagged as restricted and processing, including editing, prevented.

Where the data has been shared with others, reasonable efforts should be made to inform each recipient of the restriction. If asked to, we must also inform the person making the request about these recipients.

In cases where the restriction is lifted, the relevant individual must be informed.

The right to data portability

Data subjects have the right to obtain their data and reuse it for their own purposes, including transferring it to other organisations. This information will be provided without charge. The right to data portability applies only where all three of the following conditions are met:

- The data requested is that which the data subject has already supplied to us

- The lawful basis for processing is 6(1)(a) ‘consent’ or 6(1)(b) ‘for the performance of a contract’
- Processing is carried out by automated/electronic means

Data must be provided in a structured, commonly used, and machine-readable format (e.g. a CSV file). Assistance with this may be sought from the IT department if necessary. Where technically feasible and requested, information should be transmitted directly to another organisation.

Where the information requested concerns more than one person, the potential impact on those people must be assessed before disclosure.

The right to object

Data subjects have a limited right to object to us processing their personal data where our lawful basis is 6(1)(e) ‘necessary for the performance of a public interest task’ or 6(1)(f) ‘legitimate interests.’ Individuals may not make a general objection but must object on specific ‘grounds relating to his or her particular situation’.

When receiving an objection in these circumstances, we will cease processing unless either of the following conditions obtains:

- There are compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the objector.
- The processing is for the establishment, exercise or defence of legal claims.

In the former case, the compelling legitimate grounds must be demonstrated and not merely asserted, and this assessment must be recorded and supplied to the objector.

Data subjects must be informed of their right to object at the point of first communication and in the St Helena Transparency Notice. This right should be explicitly brought to their attention and must be presented clearly and separately from any other information.

Rights relating to automated decision-making including profiling

Automated individual decision-making is a decision made by automated means without any human involvement. Automated individual decision-making does not have to involve profiling, although it often will do. (UK)GDPR Article 4(4) defines profiling as

St Helena does not carry out automated decision making or profiling. If ever it is proposed to change this, a full Data Protection Impact Assessment (DPIA) will need to be carried out first.

These rights in practice

None of these rights is absolute but St Helena has a duty to facilitate any data subjects' rights.

The availability of these rights to data subjects is determined by the lawful base upon which we collect and process data. There are six lawful bases for processing, as laid out in Article 6(1) of the (UK)GDPR. These are:

A. Consent – we process a subject's data because they have given us their clear, unambiguous prior consent.
B. Contract – we need to process the data to enter into or fulfil a contract with the data subject.
C. Legal obligation – we process the data because the law requires us to do so.
D. Vital interests – we process the data because it is necessary to protect a specific person's life.
E. Public task – we process the data as part of our function as a public authority.
F. Legitimate interests – we process the data because we have a justifiable, reasonable purpose for doing so.

Depending on the lawful basis we use, certain rights are not available. Where there is doubt as to the lawful basis for processing, staff should consult the Record of Processing Activities and the Data Protection Officer. As a general guide, however, please note the following points:

For patient care, our lawful basis is Article 6(e); we operate as a public authority, regulated by statute. Our lawful basis for collecting special category data (sensitive medical data and similar) is (UK)GDPR Article 9(2)(h). This restricts the rights available to data subjects.

- Right to be informed
- Right of access
- Right to rectification
- Right to object

In this area, subjects do not have the right to erasure, restriction or data portability. Rights relating to profiling are not relevant to Patient and Family Services.

For St Helena's commercial operations (Fundraising, Marketing, and Lottery), our lawful bases will be a combination of legitimate interests, contract, and consent.

For electronic marketing, we are obliged by the Privacy and Electronic Communications Regulations to use prior consent as our lawful basis. This means that people have an absolute right to object. If they do so, we must cease sending any electronic marketing information immediately.

For payroll and human resources, our lawful basis for most activity will be our legal obligations to comply with employment and tax laws.