Subject Access Request Policy

Introduction

The General Data Protection Regulations gives individuals the right to know what information is held about them. It also provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with six principles (Article 5 of the GDPR), which make sure that personal information is:

a) processed lawfully, fairly and in a transparent manner
b) collected and processed for specified, explicit and legitimate purposes and not further processing in a manner that is incompatible with those purposes
c) Adequate, relevant, and limited to what is necessary for the purpose
d) Accurate and kept up to date
e) Not kept for longer than is necessary and subject to appropriate technical and organisation measures to safeguard the rights and freedoms of individuals
f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing

Secondly, it provides individuals with important rights: -

1) Right to be informed
2) Right of access
3) Right to rectification
4) Right to erasure (right to be forgotten)
5) Right to restrict processing
6) Right to data portability
7) Right to object
8) Rights related to automated decision making including profiling

2. Purpose

This document sets out our policy for responding to subject access requests under GDPR in light of the rights and responsibilities of those dealing with personal data, as decreed by the regulations. All staff are contractually bound to comply with GDPR and other relevant policies.

3. Trust policy

The John Muir Trust (the ‘Trust’) welcomes the rights of access to information that are set out in the GDPR. We are committed to operating openly and to meeting all reasonable requests for information that are not subject to specific exemption in the Act.

4. How do you make a subject access request?

A subject access request is a written request for personal information (known as personal data) held about you by the Trust. Generally, you have the right to see what personal information we hold about you, you are entitled to be given a description of the information, what we use it for, who we might pass it onto, and any information we might have about the source of the information. However, this right is subject to certain exemptions that are set out in the GDPR.

5. What is personal information?

Personal data is information that relates to a living individual who can be identified from the information and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

- an individual's salary or other financial information
- information about an individual's family life or personal circumstances, employment or personal circumstances, any opinion about an individual's state of mind
- special category personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, genetics, biometrics, physical or mental health, sexual orientation, and membership of a trade union.

What do we do when we receive a subject access request?

Checking of identity

We will first check that we have enough information to be sure of your identity.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act on their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 16, we will need to consider whether the child can provide their consent to you acting on their behalf.

Should you make a data subject access request but you are not the data subject, you must stipulate the basis under the GDPR that you consider makes you entitled to the information.

Collation of information

We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual

or electronically held information and identify any information provided by a third party or which identifies a third party.

When responding to a subject access request that involves providing information that relates both to the individual making the request and to another individual we do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- The other individual has consented to the disclosure; or
- It is reasonable in all the circumstances to comply with the request without that individual's consent

We may sometimes be able to disclose information relating to a third party and the decision will be on a case by case basis. The decision to disclose will be based on balancing the data subject's right of access against the third party's individual rights in respect of their own personal data. If the third-party consents to disclosure then it would be unreasonable not to do so. However, if there is no consent, we will decide whether it is *'reasonable in all the circumstances'* to disclose the information and will consider the following:

- Is there any duty of confidentiality owed to the third-party;
- Any steps we have taken to try and obtain third-party consent;
- Whether the third-party is capable of giving consent; and
- Any stated refusal of consent by the third-party.

Before sharing any information that relates to third parties, we may anonymise information that identifies third parties not already known to the individual and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document.

Issuing our response

Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at the John Muir Trust's office at Tower House, Station Road, Pitlochry, PH16 5AN.

We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

Will we charge a fee?

The GDPR does not allow us to charge a fee except when further copies are requested, we may charge a reasonable fee based on administrative costs.

What is the timeframe for responding to subject access requests?

We have 30 calendar days starting from when we have received all the information necessary to identify you, to identify the information requested, to provide you with the information or to provide an explanation about why we are unable to provide the information.

In many cases, it will be possible to respond in advance of the 30-calendar day target and we will aim to do so where possible.

Are there any grounds we can rely on for not complying with a subject access request?

Previous request

If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

Exemptions

The Act contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Possible exemptions would be to safeguard:

- National security
- Defence
- Public security
- The prevention, investigation, detection, or prosecution of criminal offences
- Other important public interests, economic or financial interests, including budgetary and taxation matters, public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- The protection of the individual, or the rights and freedoms of others
- The enforcement of civil law matters.

What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction.

If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

Our complaints procedure

If you are not satisfied by our actions, you can seek recourse through our internal complaints procedure, the Information Commissioner or the courts.

The Trust will deal with any written complaint about the way a request has been handled and about what information has been disclosed.

Complaints can be made to the GDPR support team at jmt.privacy@johnmuirtrust.org or:

GDPR Support
Tower House
Station Road
Pitlochry
PH16 5AN

If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner's Office ('ICO').

The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT

Tel: 0303 123 1113

https://ico.org.uk/