# Data Protection Policy


# Data Protection Policy

**Version:** **2_0**
**Owner:** **Governance & Legal**
**Approved:** **Executive October 2018**

# Data Protection Policy

**CONTENTS** **PAGE NUMBER**

# Data Protection Policy

## 1. Purpose and Scope

1.1 To operate efficiently, the Park Authority must collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, we may be required by law to collect and use information to comply with the requirements of government.

1.2 The Park Authority regards respect for the privacy of individuals and the lawful and careful treatment of personal information as very important to its successful operations and to maintaining confidence between the Park Authority and those with whom it carries out business. The Park Authority will ensure that it treats personal information lawfully and proportionately.

1.3 To this end the Park Authority will protect the rights and privacy of individuals in accordance with the Data Protection Act 2018 and the General Data Protection Regulations.

1.4 This Policy applies to all employees and Board Members as well as consultants, volunteers, contractors, agents or any other individual performing a function on behalf of the Park Authority.

## 2. Definitions of Personal Data

2.1 Personal Data

This is data which relates to a living individual ("data subject") who can be identified:

- From the data or
- From the data and other information which is in the possession of, or is likely to come into the possession of the Park Authority as the data controller.

This includes the name, address, telephone number, national insurance number as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2.2 Special Category Data

This is personal data consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

# Data Protection Policy

## 3. Data Controllers and Processers

Processing
The definition of processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

Data Controller
A Data Controller is a person or organisation who decides how any personal information can be held and processed, and for what purposes. The Park Authority is a Data Controller.

Joint Data Controllers
These are people or organisations (for example, Glasgow City Council and Police Scotland) who jointly process and share information with the Park Authority.

Data Processor
This role is carried out by any person other than a Park Authority employee (for example, contractors and agents) who process personal information on behalf of the Park Authority.

Processing Personal Information
The Park Authority will hold and process personal information only to support those activities it is legally entitled to carry out.
The Park Authority may on occasion share personal information with other organisations. In doing so, the Park Authority will comply with the provisions of the Information Commissioner's Data Sharing Code of Practice or subsequent relevant guidance.

## 4. Roles and Responsibilities

### 4.1 Information Asset Owners

The Information Asset Owners (IAOs) are the members of the Executive Team: Their role is to understand what information is held by their service, what is added and what is removed, how information is moved, and who has access and why.

Overall responsibility and accountability for ensuring that all staff and associated third parties comply with information legislation, this policy and associated procedures, lies with the senior management team comprising:

- Chief Executive
- Director of Corporate Services
- Director of Rural Development and Planning
- Director of conservation & Visitor Operations
- Head of Communications

### 4.2 Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Park Authority and its employees about their obligations to comply with the Data Protection Act 2018 and associated guidance from the UK Information Commissioner.

- Monitor compliance with the Data Protection Act, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.
- Provide advice about data protection impact assessments and monitor their performance;
- Co-operate with the supervisory authority (the Information Commissioner's Office).
- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

4.3 ICT Systems Manager

The ICT Systems Manager is responsible for creating, implementing and maintaining ICT security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance.

4.4 Individual Members of Staff and Elected Board Members

Individual members of staff and elected Board members are responsible for protecting personal information held or processed on computer, or held in paper records in their care.

## 5. Lawful Basis for Processing Personal Information

5.1 The lawful bases for processing personal data are set out below. At least one of these must apply whenever we process personal information:

- **Consent**: an individual has given clear consent for us to process his/her personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract that we have with the individual, or because the individual has asked us to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public interest**: the processing is necessary for us to perform a task in the public interest or in the exercise of official authority vested in the Park Authority.
- **Legitimate interests**: the processing is necessary for the purposes of legitimate interests pursued by us or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by us in the performance of our official tasks: it can only apply to us when it is fulfilling a different role.

## 6. Rights of Individuals

The Data Protection Act 2018 provides individuals with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Park Authority to correct any inaccuracies.

- The right to request the erasure of any personal information held by the Park Authority where the Park Authority no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Park Authority processing their personal information.
- Rights in relation to automated decision making and profiling.

## 7. The Data Protection Principles

There are seven principles for the processing of personal information which are legally binding on the Park Authority. Personal information must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of the data subject.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The Data Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

## 8. Consent

When we process personal data we will explain the following:

- Exactly why we are asking for the personal data
- What we are going to do with the data
- How long we will hold the data
- State if there is any other organisation that we will be asking to process the data
- How to withdraw consent if you no longer want us to process your data
- We will seek positive opt in to consent to our use of personal data
- We will give options to consent separately if we need to process personal data for more than one purpose

Please send any enquiry about our use of your personal data to:

Data Protection Officer
Loch Lomond & The Trossachs National Park Authority

# Data Protection Policy

Carrochan
Carrochan Road
Balloch
G83 8EG

Or you can email us: info@lochlomond-trossachs.org

## 9. Using your Right of Access

9.1 You have the right to access the personal data the Park Authority holds about you. This right is called a Subject Access Request, often referred to as a SAR.

You can receive a copy of your personal data held by the Park Authority, details on why it is being used, who it has been/will be shared with, how long it will be held for, the source of the information and if the Park Authority uses computer systems profiling to take decisions about you. Details on how to submit a Subject Access Request can be found on our website at:

http://www.lochlomond-trossachs.org/park-authority/freedom-of-information/accessing-personal-information/

9.2 Your request should include a contact address and documentary evidence of your identity (e.g. copies of your driving licence, passport or birth certificate). Please don't send us original documents. Please also provide as many details as possible about the information you're asking for. If we need more information to help find your information or confirm your identify you, we will ask. When we have all the necessary information, your request will be processed and a response will be sent to you within one calendar month.

9.3 If your request is very complex we can extend the deadline for responding by a further two months. If this is necessary we will tell you about this and provide an explanation and revised deadline for completing your request, within one month of receiving your request.

9.4 If your request is considered to be excessive or unfounded, especially if you have submitted a series of similar requests, we can either refuse your request or charge a fee. If this is the case we will provide you with an explanation of this and give you the opportunity to complain about our decision.

## 10. Notifying the Information Commissioner

The Park Authority must advise the Information Commissioner's Office that it holds personal information about living people. It must also notify the Information Commissioner should a notifiable data breach occur.

# Data Protection Policy

## 11. Complaints

The UK Information Commissioner (ICO) is the final stage for complaints about data protection matters. If an individual is dissatisfied with the Park Authority's handling of their personal data, they can ask the ICO to look at your complaint, however The ICO cannot normally look at complaints which have not first been investigated through the Park Authority's complaints handling procedure.

Details of our complaints process can be found on our website at:
http://www.lochlomond-trossachs.org/park-authority/how-to-make-a-complaint/

Details of how to make a complaint to the ICO can be found at:
https://ico.org.uk/make-a-complaint/

## 12. Further Information and Guidance

Data Protection Officer
National Park Authority
Carrochan
Carrochan Road
Balloch
G83 8EG

E-mail: info@lochlomond-trossachs.org

Tel: 01389 722600

Further information is also available from the Information Commissioner's website

## 13. Equality and Diversity Impact Assessment

An equality and diversity impact assessment was carried out and no discriminatory effects were identified for any particular group within the workforce. This will be monitored on an ongoing basis. We are committed to making our services easy to use for all members of the community. In line with our statutory equalities duties, we will always ensure that reasonable adjustments are made to help customers access and use our services. If you want this information in another language or format, such as large font, please ask us and we will do our best to help meet your requirements.

## 14. Best Value

The policy meets the best value criteria, specifically in terms of governance and accountability. As a public authority we are required to comply with our statutory obligations under the legislation, with appropriate policies and procedures in place to process personal information in accordance with the rights of individuals.

# Data Protection Policy

**Appendix 1**

**Policy statement and additional safeguards on processing special category data and personal data relating to criminal convictions and offences**
**Introduction**

Data Controllers who process Special Category personal data, or personal data relating to criminal convictions and offences under various parts of the Data Protection Act 2018 are required to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

More specifically, the law states that:

"The controller has an appropriate policy document in place in relation to the processing of personal data… if the controller has produced a document which—

a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and

b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained."

This Appendix 1 to the Park Authority's Data Protection Policy is our response to this requirement.

**Context**

Special Category Data is defined in Article 9(1) as data which identifies:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data (new); and
- biometric data where processed to uniquely identify a person.

Additionally, whilst not deemed Special Category Data, special conditions apply to the processing of Personal Data regarding Criminal Convictions and Offences.

Processing of Special Category Data is prohibited unless one of the following conditions applies:-

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Additionally for Criminal Convictions and Offences processing is only permitted:-

> "under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

**Policy Statement**

1. Lawfulness, fairness and transparency:
   Data flows into and out of the Park Authority are being assessed to determine the legal basis under which that data is processed. This process has resulted in an understanding of the information we hold, its purpose, our basis for holding it, who provides us with it and who we provide it to in turn. We are satisfied that we will have a legal basis for holding the personal data we hold, and that we will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices have been drafted to reflect the legal basis of processing. Our principal privacy notice and other information on privacy and use of data is available at: http://www.lochlomond-trossachs.org/privacy-cookie-policy/

# Data Protection Policy

2. Purpose limitation:
The purposes for which data are collected are clearly set out in the relevant privacy statements. This includes reference to further use of data for internal management information purposes.

3. Data minimisation:
The Park Authority is undertaking critical examination of the data sets they hold and are actively seeking to reduce superfluous and/or obsolete data and data sets, and will cease collection of any personal data that is not required for the purposes for which the Park Authority has no reasonable rights or purpose in pursuance of its functions.

4. Accuracy:
The Park Authority will continually check data for accuracy and, where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5. Storage limitation:
The Park Authority will only keep personal information for periods found in our Records Retention and Disposal Schedules. Sometimes this time period is set out in the law, but in most cases it is based on business need. Further information on record retention is available on request from info@lochlomond-trossachs.org.

Ongoing management of the council's records and information is subject to the provisions of our Records Management Policy and our Records Management Plan which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. The Records Management Plan sets out, in much greater detail, the provisions under which the Park Authority complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6. Integrity and confidentiality:
The Park Authority has relevant information security policies and procedures in place which set out roles and responsibilities within the organisation in relation to information security. Our ICT systems have appropriate protective measures in place incorporating defense in depth and relevant systems are subject to external assessment and validation.

# Data Protection Policy

**Document Control Sheet** **Appendix B**

| | |
|---|---|
| **Prepared By** | Governance and Legal Team |
| **Date Effective From** | October 2018 |
| **Review Frequency** | As required to comply with data protection legislation |
| **Contact** | Governance and Legal Team |

**Revision History:**

| Version: | Date: | Summary of Changes: | Name: |
|---|---|---|---|
| 2_0 | October 2018 | Policy re-written to comply with new data protection legislation | Information Officer |
| 1_0 | April 2014 | New Policy | Jaki Carnegie |

**Approvals:** This document requires the following signed approvals.

| Name/Title | Date | Version |
|---|---|---|
| Executive Team | October 2018 | 2_0 |
| Jaki Carnegie | April 2014 | 1_0 |

**Distribution:** This document has been distributed to

| Name: | Title/Division: | Date of Issue: | Version: |
|---|---|---|---|
| All staff | All staff | October 2018 | 2_0 |
| All staff | All staff | May 2014 | 1_0 |