| Lee Valley Regional Park Authority | Agenda Item No: |
|---|---|
| **LEE VALLEY REGIONAL PARK AUTHORITY** | 9 |
| **AUTHORITY MEETING** | Report No: |
| **19 JANUARY 2023 AT 14:00** | A/4327/23 |

# DATA PROTECTION POLICY

Presented by the Deputy Chief Executive

## SUMMARY

This report seeks Member approval for the revised policy relating to data protection, which has been updated as part of the ongoing review of all the Authority's existing policies. The policy has been updated to align with the Information Commissioner's Accountability Framework.

The Executive Committee considered the updated policy at its meeting on 17 November 2022 (Paper E/783/22) and recommended it to the Authority subject to one amendment, which has been made and the detail is set out at paragraph 9 of the report.

## RECOMMENDATION

Members Approve: (1) the draft Data Protection Policy attached as Appendix A to this report.

## BACKGROUND

1 The Authority has a register of policies that ensure the organisation works efficiently and consistently towards delivering its Business Strategy. These policies are reviewed to ensure that they are relevant and up to date with legislation and best practice.

2 One of these policies is the Data Protection Policy, which sets out the Authority's approach towards ensuring that it complies with its legal obligations under the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 in respect of personal data that it holds and processes.

3 It should be noted that the Authority implements legislative changes from the date that they are introduced and there may be a time lag between this and the relevant policies being updated.

## DATA PROTECTION POLICY

4 A draft of the Data Protection Policy is attached as Appendix A to this report for Members' consideration and approval.

5 The Data Protection Policy is intended to ensure that the Authority complies fully with its legal obligations under the UK GDPR and Data Protection Act 2018 and maintains the confidence of everyone who trusts it with their personal data. The current policy was introduced in April 2018 to comply with the General Data Protection Regulation 2018 and the then forthcoming Data Protection Act 2018 (Paper E/558/18).

6 The draft Data Protection Policy has been fully updated to align with the Information Commissioner's Office (ICO) Accountability Framework. The Accountability Framework sets out the ICO's expectations of steps organisations should take to demonstrate their compliance with and accountability for data protection law.

7 Section 15 of the draft Data Protection Policy refers to a number of procedures and supporting documents. These will be reviewed to ensure alignment with the ICO's Accountability Framework during the next 3-4 months.

8 The Data Protection Policy provides for the Head of Legal Services to fulfil the role of Data Protection Officer (DPO). The current DPO is the Deputy Chief Executive. The DPO has a formal role under UK GDPR, they are responsible for monitoring compliance, informing and advising on data protection obligations and acting as a contact point for data subjects and for the ICO.

9 The Executive Committee considered the updated policy at its meeting on 17 November 2022 (Paper E/783/22) and recommended it to the Authority subject to one amendment, which has been made. This was to provide that significant data protection breaches are reported to the Chair of the Authority and to the Chair of the Audit Committee. The change has been made to paragraphs 11.6 and 12.1 of the draft policy attached and is highlighted in yellow.

## ENVIRONMENTAL IMPLICATIONS

10 There are no environmental implications arising directly from the recommendations in this report.

## FINANCIAL IMPLICATIONS

11 There are no financial implications arising directly from the recommendations in this report.

## HUMAN RESOURCE IMPLICATIONS

12 There are no human resource implications arising directly from the recommendations in this report.

## LEGAL IMPLICATIONS

13 The Policy supports the Authority in meeting its obligations under UK GDPR and the Data Protection Act 2018.

## RISK MANAGEMENT IMPLICATIONS

14 The Authority's Corporate Risk Register includes the risk of failure to comply

with the Lee Valley Regional Park Act 1966 and other statutory requirements (SR1.1). The Data Protection Policy aims to mitigate the risk that the Authority fails to comply with its legal obligations under data protection law.

## EQUALITY IMPLICATIONS

15 There are no equality implications arising directly from the recommendations in this report.

---

Author: Julie Smith, 01992 709838, jsmith@leevalleypark.org.uk

## APPENDIX ATTACHED

| | |
|---|---|
| Appendix A | Draft Data Protection Policy |

## ABBREVIATIONS

| | |
|---|---|
| DPO | Data Protection Officer |
| ICO | Information Commissioner's Office |
| UK GDPR | Regulation (EU) 2016/679 as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 |

## PREVIOUS COMMITTEE REPORT

| | | | |
|---|---|---|---|
| Executive | E/783/22 | Data Protection Policy | 17 Nov 2022 |
| Executive | E/558/18 | GDPR and Data Protection Policy | 26 April 2018 |

This page is blank

Lee Valley
Regional Park Authority

# Data Protection Policy

## [January 2023]

Reference: Version 2

This document is controlled by Lee Valley Regional Park Authority.

**Lee Valley Regional Park Authority,**
Myddelton House, Bulls Cross,
Enfield, Middlesex, EN2 9HG

THIS PAGE IS INTENTIONALLY BLANK

## Document Information

**Title:** **Data Protection Policy**

**Status:** Draft

**Current Version:** v2.00

| | |
|---|---|
| **Authors** | Rajan Mistry, Legal & Information Officer<br>rmistry@leevalleypark.org.uk<br>☎ (01992) 709869<br><br>Julie Smith, Head of Legal Services<br>jsmith@leevalleypark.org.uk<br>☎ (01992) 709838 |
| | |
| **Sponsor** | Beryl Foster, Deputy Chief Executive<br>bfoster@leevalleypark.org.uk<br>☎ (01992) 709836 |
| | |
| **Consultation:** | Policy & Procedure Review Group<br>Senior Management Team |
| | |
| **Approved** | **Approved by:** Authority<br>**Approval Date:** [January 2023]<br><br>**Review Frequency:** Every three years or earlier if there is a change in legislation<br><br>**Next Review:** January 2026 |

| **Version History** | | |
|---|---|---|
| **Version** | **Date** | **Description** |
| 1 | 25 August 2020 | |
| 2 | [January 2023] | Updated to align with the Information Commissioner's Office Accountability Framework |

## Contents


| **Preliminary Pages** | **Page** |
|---|---|
| Title Page | 1 |
| Document Creation and Approval | 3 |
| Document History | 3 |
| Contents | 3 |

| Main Body | | |
|---|---|---|
| **Section** | **Title** | **Page** |
| 1 | Background | 5 |
| 2 | Purpose | 5 |
| 3 | Scope | 5 |
| 4 | Data Protection Principles | 6 |
| 5 | Individuals' Rights | 6 |
| 6 | Transparency | 7 |
| 7 | Records of processing and lawful basis | 8 |
| 8 | Contracts and data sharing | 10 |
| 9 | Data Protection by design and default | 11 |
| 10 | Records management and security | 11 |
| 11 | Breach response | 12 |
| 12 | Responsibilities | 13 |
| 13 | Training and awareness | 14 |
| 14 | Monitoring | 14 |
| 15 | Relevant Policies and Procedures | 14 |

## 1. Background

1.1 The Authority has legal obligations in respect of how it treats personal data that it holds and processes under the UK General Data Protection Regulations (UK GDPR), as tailored by the Data Protection Act 2018. The UK GDPR is Regulation (EU) 2016/679 as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.2 It is essential that the Authority fulfils these obligations if it is to maintain the confidence of those providing it with personal data, including attendees at Park events, users of Park facilities, those subscribing to receive updates and information about the Park, volunteers, employees and Members.

1.3 If the Authority does not meet its obligations in respect of data protection it could suffer reputational damage. It could also receive a significant fine. A breach of the UK GDPR can lead to a fine of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher.

## 2. Purpose

2.1 This policy is in place to ensure that the Authority complies fully with its legal obligations under the UK GDPR and Data Protection Act 2018 and maintains the confidence of everyone who trusts it with their personal data.

## 3. Scope

3.1 This policy applies to all personal data that is held and processed by the Authority, however it is stored – physically or electronically - and whoever the person is to who it relates – employee, worker, volunteer, someone attending an event or otherwise using the Park or any other person.

3.2 Personal data is any information that relates to an identified or identifiable individual. Examples of personal data include names and addresses, e-mail addresses and banking details.

3.3 Certain personal data is more sensitive and is special category data. This includes:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

- genetic data;
- biometric data; and
- data concerning a person's health, sex life and sexual orientation.

3.4 The policy applies to all Authority staff and to all activities undertaken by the Authority that involve the use of personal data.

## 4. Data Protection Principles

4.1 The Authority is responsible for its use and processing of personal data. It will comply with the data protection principles that are set out in the UK GDPR. These require that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate 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;
- 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.

4.2 The Authority will appoint a Data Protection Officer (DPO) to oversee its arrangements for complying with the UK GDPR. The DPO will be independent, an expert in data protection, adequately resourced and report to the highest management level.

## 5. Individuals' rights

5.1 The Authority will ensure that individuals are able to exercise their rights under UK GDPR. These are the rights:

- to be informed about collection and use of their personal data;
- to access and receive a copy of personal data held by an organisation (commonly referred to as a subject access request);
- to have inaccurate personal data rectified or completed if it is incomplete;
- to have personal data erased;
- to request restriction of the processing of their personal data;
- to obtain and reuse their personal data for their own purposes across different services;
- to object to the processing of their personal data in certain circumstances; and
- relating to automated decision making including profiling.

5.2 The Authority will ensure that individuals are informed about their rights and how to exercise them.

5.3 Requests from individuals about their rights will be responded to by the Legal & Information Officer in accordance with the procedure for subject access requests and exercise of individuals' UK GDPR rights.

5.4 If individuals wish to complain about the use of their personal data they may complain to the DPO. They also have a right to complain to the ICO.

## 6. Transparency

6.1 The Authority will be open and honest about all aspects of its management of personal data.

6.2 Privacy notices will be provided at the point at which personal data is collected, for example when booking an activity or joining a mailing list.

6.3 Privacy notices will provide all the information that is required by UK GDPR:

- the Authority's contact details and the DPO's contact details;

- the purposes of the processing and the lawful bases (and, if applicable, the legitimate interests for the processing);
- the types of personal data you obtain and the data source;
- details of all personal data that the Authority shares with other organisations;
- retention periods for the personal data, or the criteria used to determine the period;
- details about individuals' rights including, if applicable, the right to withdraw consent and the right to make a complaint; and
- details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable).

6.4 Privacy notices will be clear and easy to understand. They will be reviewed periodically to ensure that they stay accurate, up to date and effective.

6.5 Where the Authority obtains personal data from a source other than the individual to which it relates it will provide privacy information within one month of obtaining the data.

## 7. Records of processing and lawful basis

7.1 The Authority will maintain a comprehensive record of processing activities that ensures it knows what personal data it holds, where it is and what it does with it.

7.2 The record of processing activities will include all the information required under the UK GDPR including:

- a description of the categories of individuals and of personal data;
- the purpose of processing;
- the categories of recipients of personal data;
- retention schedules; and

- description of technical and organisational security measures in place.

It will include processing activities carried out on behalf of the Authority. The Authority will review the record of processing activities regularly to ensure that it remains accurate and up to date.

7.3 The Authority will only process personal data where it has a lawful basis for doing so. The lawful bases for processing are:

- consent – an individual has given consent to process their personal data for a specific purpose;
- contract – the processing is necessary in order to fulfil a contract or prior to entering into a contract;
- legal obligation – the processing is needed to comply with the law;
- vital interest – the processing is necessary to protect someone's life;
- public task – the processing is necessary to perform a task in the public interest or to fulfil an official function and has a clear basis in law; and
- legitimate interests – the processing is necessary for an organisation's legitimate interests or those of the third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

7.4 The Authority will document and appropriately justify the lawful basis for processing personal data. This information will be made publicly available through inclusion in privacy notices and will be easy to access and understand.

7.5 Where the basis of processing is consent, requests for consent will:

- be kept separate from other terms and conditions;
- require a positive opt-in and will not use pre-ticked boxes;
- be clear and specific;
- not be a pre-condition of signing up to a service;
- explain how to withdraw consent; and

- provide the name of the Authority and any other party that that the information may be shared with.

7.6 For children under the age of 13, parents or guardians will be asked to provide consent on behalf of their child. For children who are 13 years or over, they will be asked to provide their own consent unless factors suggest that they are unable to give informed consent in which case a parent or guardian's consent will be required.

7.7 The Authority will maintain easily accessible records of what an individual has consented to and will update those records if an individual withdraws their consent. Consent records will be reviewed and refreshed periodically.

7.8 Where the basis for processing is legitimate interests then an appropriate legitimate interest assessment will be completed prior to starting the processing. The legitimate interest assessment will assess the benefits of the processing and whether it is necessary.

## 8. Contracts and data sharing

8.1 The Authority will only share personal data with third parties where this is necessary to achieve a clearly defined and specific purpose and it is permitted to do so under the UK GDPR.

8.2 The Authority will ensure that before deciding to share data or entering into an arrangement for a third party to process data on its behalf, a data privacy impact assessment is carried out to assess the benefits and risks of sharing personal data and that the Authority is legally permitted to do so.

8.3 Where data sharing is to take place, there will be a written data sharing agreement that explains the purpose for the sharing and each parties' responsibilities for the personal data that is shared. There will be regular reviews of how the agreement is working.

8.4 Any processing of personal data by third parties on behalf of the Authority will be in accordance with a data processing agreement or other contract that meets the requirements of UK GDPR. The Authority will make appropriate arrangements to carry out due diligence checks on third parties processing personal data that are proportionate to the risk of the processing and to check compliance with contractual obligations relating to data protection.

8.5 The Authority will not transfer personal data outside of the European Economic Area (EEA) unless the UK has in place adequacy regulations in respect of the country or territory to which a transfer is to be made or appropriate safeguards can be put in place.

8.6 The procedure for data sharing and processing of data by third parties provides further information and detail as to how the Authority will ensure any sharing and processing of data is in accordance with the UK GDPR.

## 9. Data Protection by design and default – risks and data protection impact assessments

9.1 The Authority will identify, assess and manage risks relating to personal data in accordance with its risk management processes. Any risks that are identified will be recorded in its information asset register, corporate risk register and departmental and venue risk registers as appropriate.

9.2 The Authority will adopt a data protection by design and by default approach to managing risks. It will proactively consider data protection risks and issues as part of the design and implementation of its systems, projects and activities.

9.3 At the outset of any project, new activity or sharing of personal data, a decision will be taken as to whether a data protection impact assessment (DPIA) is required and if it is required the DPIA will be carried out at the start of the project, new activity or sharing of data.

9.4 The DPIA will be used in the design of the project, activity or data sharing to ensure that appropriate and effective action is taken to mitigate and manage any risks that it identifies.

9.5 The Data Protection Impact Assessment procedure provides further detail when a DPIA is required and its preparation and implementation.

## 10. Records management and security

10.1 The Authority will put in place procedures to ensure good records management. It will maintain an information asset register that records all assets, systems and applications used for processing or storing personal data. It will conduct regular reviews of records containing personal data to make sure they are accurate, adequate and not excessive.

10.2 The Authority will keep in place a retention schedule outlining storage periods for all personal data, which will be reviewed regularly. When it is time for records containing personal data to be destroyed they will be destroyed in accordance with the records retention & disposal procedure.

10.3 The Authority will have in place information security measures to ensure that personal data is held and transferred securely.

10.4 The Authority will have in place an acceptable use policy governing the use of software that processes or stores information. Access to personal data will be restricted to authorised staff that need to access the data to fulfil their roles. The Authority will prevent unauthorised access to systems or applications processing personal data. It will manage the security risks of using devices, home or remote working and removeable media.

10.5 The Authority will secure its premises to prevent unauthorised physical access, damage and interference to personal data. Paper records containing personal data will be securely stored.

10.6 The Authority will maintain a business continuity plan that enables it to manage disruption and protects against the loss of personal data.

## 11. Breach response

11.1 The Authority will have in place a breach response procedure that sets out the procedure to be followed in the event of a suspected data protection incident. A data protection incident includes any instance in which personal data has or may have been passed to any person that should not have access to it.

11.2 Any member of staff who suspects that there has been a data protection incident and breaches, however minor, must report the incident to the Legal & Information Officer and to the DPO immediately.

11.3 The Legal & Information Officer and DPO will manage the response to data protection incidents. This will include prompt notification of affected individuals where a data protection breach is likely to result in a high risk to their rights and freedoms.

11.4 The DPO will assess the incident and will decide whether it needs to be reported to the ICO. If the incident needs to be reported, the DPO will ensure that the report is made within 72 hours of the Authority first becoming aware of it.

11.5 A log will be kept of all data protection incidents that records information about near misses or breaches. The log will also document the reasons for concluding that incident does not need to be reported to the ICO. Where an incident does occur, it will be reviewed to identify what lessons can be learned and steps to be taken to prevent a similar incident from occurring in the future.

11.6 The DPO will report significant data protection breaches to the Chair of the Authority and the Chair of the Audit Committee, who will consider whether the Executive Committee and/or the Audit Committee and/or full Authority should be informed of and should formally consider the data protection breach.

## 12. Responsibilities

12.1 The Chair of the Authority and Chair of the Audit Committee will have overall oversight of this policy and will ensure that significant data protection breaches are reviewed, if appropriate, by the relevant Committee so that appropriate actions are taken to minimise the risk of a future similar breach.

12.2 The Data Protection Officer (DPO), who will be the Head of Legal Services, is responsible for:

- informing and advising on the Authority's obligations to comply with the UK GDPR and other data protection laws;
- monitoring compliance with UK GDPR and this data protection policy;
- managing responses to data protection incidents;
- raising awareness of data protection issues and training staff;
- advising on and monitoring data protection impact assessments and legitimate interest assessments;
- co-operating with the ICO; and
- acting as first point of contact for the ICO and for individuals whose data is processed.

12.3 The Legal & Information Officer is responsible for supporting the DPO in their role and in particular for:

- co-ordinating the information asset register;
- managing responses to subject access requests and other requests from individuals to exercise their individual rights;
- supporting the DPO in managing responses to data protection incidents;
- maintaining a log of data protection incidents;

- providing advice and assistance to colleagues on the carrying out of legitimate interest assessments and data privacy impact assessment; and

- providing advice and assistance to colleagues on what they need to do to comply with this data protection policy and with relevant procedures.

12.4 All staff are responsible for ensuring that they understand and apply this policy and associated procedures in carrying out their roles. They are in particular responsible for:

- ensuring the information asset register is kept up to date in respect of any personal data for which they are owner and that retention schedules are adhered to;

- assisting the Legal & Information Officer with subject access requests or any other request relating to exercise of an individual's rights;

- where they are the lead for a project or activity, for ensuring that a data protection impact assessment is carried out and is implemented; and

- immediately reporting any data protection incident or suspected incident to the DPO and the Legal & Information Officer.

## 13. Training and awareness

13.1 The Authority will ensure that all its staff receive regular and appropriate training on the requirements of UK GDPR, this policy and the procedures that they need to follow.

13.2 The Authority will put in place a training programme, which includes training as part of staff induction and then regular refresher training for all staff. There will be regular awareness raising of data protection, information governance and associated policies and procedures.

## 14. Monitoring

14.1 The Authority's internal audit programme will include data protection and related information governance, for example security and records management. It will also carry out appropriate ad-hoc monitoring and spot checks.

14.2 The Authority will also make use of the ICO provided self-assessment tools to provide assurances on data protection and information security compliance.

## 15. Relevant Policies and Procedures

- Procedure for subject access requests and exercise of individuals' UK GDPR rights
- Procedure for data sharing and processing of data by third parties
- Legitimate Interests Assessment procedure
- Data Protection Impact Assessment procedure
- Records Retention & Disposal Procedure
- Privacy notices
- Information Asset Register
- Record of processing activities
- Consent review procedure
- Breach Response Procedure
- IT Usage Policy
- Business Continuity Plan
- Risk Register Procedure

This page is blank