Lee Valley Regional Park Authority	Agenda Item No:
LEE VALLEY REGIONAL PARK AUTHORITY	8
AUTHORITY MEETING	Report No:
26 APRIL 2018 AT 14:00	**A/4257/18**

GENERAL DATA PROTECTION REGULATIONS (GDPR) & DATA PROTECTION POLICY

Presented by the Director of Corporate Services

SUMMARY

The purpose of this report is to seek Members approval to the updated Data Protection Policy to ensure compliance with the General Data Protection Regulations (GDPR) and forthcoming Data Protection Act 2018 regarding the protection of personal data that the Authority holds about or concerning any individual. The Regulations were adopted on 27 April 2016 and become enforceable from 25 May 2018.

Executive Committee considered the revised Data Protection Policy for recommendation to Authority at its meeting earlier today and an oral update will be provided at the Authority meeting.

RECOMMENDATION

Members Approve: (1) the revised Data Protection Policy as set out in Annex A to this report (Paper E/558/18).

BACKGROUND

1 The Authority's officers have revised the Data Protection Policy (which was last updated in March 2013) to ensure that Lee Valley Regional Park Authority (LVRPA) complies fully with its legal obligations under the General Data Protection Regulations (GDPR) and forthcoming Data Protection Act 2018 regarding handling of the personal data of its customers, suppliers, employees, workers and other third parties.

SUMMARY OF THE POLICY

2 The aim of the policy is to ensure all employees or partner organisations (suppliers and contractors) which collect, store, access or otherwise process personal data on behalf of the Authority are familiar with the policy and ensure that procedures within it are fully applied in relation to the handling or "processing" of personal data. It is important that employees understand their obligations under the GDPR data protection regime in relation to the personal information of customers, contractors and staff.

3 The aim of the policy is to ensure all employees or partner organisations (suppliers and contractors) which collect, store, access or otherwise process personal data on behalf of the Authority are familiar with the policy and ensure that procedures within it are fully applied in relation to the handling or "processing" of personal data. It is important that employees understand their obligations under the GDPR data protection regime in relation to the personal information of customers, contractors and staff.

4 The policy concerns personal data held by LVRPA in relation to any person.

5 For detailed summary of the policy please see Annex A to this report (Paper E/558/18.

IMPLICATIONS

6 Any environmental, financial, human resource, legal, risk management and equality implications arising directly from the recommendations in this report are detailed in Annex A to this report (Paper E/558/18).

Author: Simon Sheldon, 01992 709859, ssheldon@leevalleypark.org.uk

PREVIOUS COMMITTEE REPORTS

Executive	E/558/18	General Data Protection Regulations (GDPR) & Data Protection Policy	26 April 2018
Authority	A/4166/13	Policy Review Update	25 April 2013

ANNEX ATTACHED

Annex A	Paper E/558/18

Lee Valley Regional Park Authority **LEE VALLEY REGIONAL PARK AUTHORITY** **EXECUTIVE COMMITTEE** **26 APRIL 2018 AT 11:00**	**Agenda Item No:** **Report No:** **E/558/18**

GENERAL DATA PROTECTION REGULATIONS (GDPR) & DATA PROTECTION POLICY

Presented by the Director of Corporate Services

EXECUTIVE SUMMARY

The purpose of this report is to seek Members approval to the updated Data Protection Policy to ensure compliance with the General Data Protection Regulations (GDPR) and forthcoming Data Protection Act 2018 regarding the protection of personal data that the Authority holds about or concerning any individual. The Regulations were adopted on 27 April 2016 and become enforceable from 25 May 2018.

RECOMMENDATION

Members Recommend to the Authority:

(1) the revised Data Protection Policy as set out in Appendix A to this report.

BACKGROUND

1 The Authority's officers have revised the Data Protection Policy (which was last updated in March 2013) to ensure that Lee Valley Regional Park Authority (LVRPA) complies fully with its legal obligations under the General Data Protection Regulations (GDPR) and forthcoming Data Protection Act 2018 regarding handling of the personal data of its customers, suppliers, employees, workers and other third parties.

SUMMARY OF THE POLICY

2 The aim of the policy is to ensure all employees or partner organisations (suppliers and contractors) which collect, store, access or otherwise process personal data on behalf of the Authority are familiar with the policy and ensure that procedures within it are fully applied in relation to the handling or "processing" of personal data. It is important that employees understand their obligations under the GDPR data protection regime in relation to the personal information of customers, contractors and staff.

3 This policy sets out the minimum standards for compliance with the GDPR and in particular, the Data Protection Principles. All individuals have a right to know

why their personal data is collected, how long it is kept, who has access to it and for what purpose and above all that they have a right to demand that we correct inaccurate information. Individuals have the right to object to their personal data being collected or 'processed'. By adopting the standards set out in this document we can be assured that our own privacy and data rights are respected and protected and we can share this reassurance with everyone we deal with.

4 The policy concerns personal data held by LVRPA in relation to any person.

5 Data Protection is monitored by the Information Commissioner's Office (ICO), an independent official body. The Commissioner has the power to fine or take legal action against organisations found to be in breach of the GDPR. Separately, the new UK Act will include provisions on directors' personal liability where an offence is committed with the consent, connivance or negligence of a director.

This policy is designed to protect LVRPA, employees, customers and partner organisations by preventing such breaches from occurring. It does not form part of an employee's contract and may be amended at any time.

6 The changes in the policy relate to a change in the names, contact details and roles of designated officers in the Authority due to organisational changes following the establishment of Lee Valley Leisure Trust Ltd (the Trust) in April 2015 and the strengthening of procedures for the collection, storage and transmission of personal data.

- The LVRPA's Data Protection Officer will now be the Director of Corporate Services.
- The regulations provide harmonisation of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations.
- The regulations add a strict data protection compliance regime with severe penalties of up to 4% of turnover.
- The regulations bring a new set of digital rights recognising the increased value of personal data in the modern world.
- The Privacy Notice requirements remain and are expanded. They must include detail of information collected specifying for what purpose and legal basis, retention time for personal data, data subject's rights to object or restrict processing, data subjects right to be forgotten, and contact information for data controller and data protection officer has to be provided.
- Subject Access Request timeframes have changed from 40 days to one month for responses.
- There are changes in breach notification, all breaches must be reported within 72 hours to the ICO.

The Trust will set out its own policy to present to its Board which will broadly reflect those of the Authority, although names and contact details will be different.

7 The Authority will act as Data Controller for data that it collects and processes, with the Trust acting as Data Processor for the data it collects or processes for the Authority.

8 Members are asked to approve the revised policy at Appendix A to this report.

ENVIRONMENTAL IMPLICATIONS

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

FINANCIAL IMPLICATIONS

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

HUMAN RESOURCE IMPLICATIONS

11 All staff will and have been taking online training sessions to ensure that there is an understanding and awareness of the issues that surround Data Protection under the GDPR regarding the protection of personal data that it holds about or concerning any individual. This issue remains high, embedding an understanding and culture across the organisation is a priority. Supporting literature will be updated to reflect these changes as well as updating the intranet to ensure a robust on-line message is maintained as well.

LEGAL IMPLICATIONS

12 The GDPR has direct effect which means that once passed it confers rights on individuals which the courts of all European Union member states have to recognise and abide by. It was passed in April 2016 for implementation from 25 May 2018 and therefore its provisions have to be complied with after this date. The Government has confirmed that the UK's decision to leave the European Union (in 2019) will not alter this position. A Data Protection Bill is currently making its way through the House of Parliament and following consideration of amendments is expected to receive Royal Assent before 25 May 2018. The GDPR affords European Member States rights to make certain changes to the rules in their particular application in individual member states. If material derogations or exemptions to the provisions of the GDPR are contained in the Data Protection Act 2018 then another report may need to be presented to Members accompanied by an updated Data Protection Policy.

RISK MANAGEMENT IMPLICATIONS

13 Risk of breach of GDPR and/or the forthcoming Data Protection Act 2018 could result in a significant fine and reputational damage.

14 To mitigate against these risks the Authority has reviewed its existing Data Protection Policy, carried out Privacy Impact Assessments covering all areas where personal data is collected, stored and processed in accordance with the guidance issued by the Information Commissioner's Office. This has resulted in the drawing up of a new Data Protection Policy which is compliant with the GDPR. The Authority also has procedures and practices laid down in relation to the conduct of Authority business.

15 Online Data Protection training is live for all those staff who process personal data so that all are aware of their responsibilities and the risk of inadvertent breach is minimised.

Author: Simon Sheldon 01992 709859, ssheldon@leevalleypark.org.uk

PREVIOUS COMMITTEE REPORTS

Authority	A/4166/13	Policy Review Update	25 April 2013

APPENDIX ATTACHED

Appendix A	The Data Protection Policy

LIST OF ABBREVIATIONS

GDPR	General Data Protection Regulations
LVRPA	Lee Valley Regional Park Authority
ICO	Information Commissioner's Office
the Trust	Lee Valley Leisure Trust Ltd (trading as Vibrant Partnerships)

Lee Valley
Regional Park Authority

Data Protection Policy

April 2018

Reference: [Version 1]

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

i Document Information

Title: **Data Protection Policy**

Status: Live

Current Version: v2.00 (March 2013)

Author	Gavin Embley, Information Officer Performance & Information Management, Business Support, Vibrant Partnerships gembley@vibrantpartnerships.co.uk ☎ (01992) 709819 or 819
Sponsor	Name – Nigel Foxall Director of Business Support nfoxall@vibrantpartnerships.co.uk ☎ (01992) 709820 or x820
Consultation:	Policy Review Group Authority Legal Team LVRPA SMT
Approved	**Approved by:** Authority Members' Committee **Approval Date:** xxxxx **Review Frequency:** Every three years **Next Review:** April 2020

Version History		
Version	**Date**	**Description**
1	6th April 2018	Updated from DPA Policy to comply with GDPR

ii Contents

Preliminary Pages		
Section	**Title**	**Page**
Cover	**Title Page**	1
i	**Document Information**	3
Ii	**Contents**	4

Main Body		
Section	**Title**	**Page**
1	Context	5
2	Policy Aims	5
3	Content	5
4	Responsibilities	8
5	Legal Considerations	8
6	Relevant Policies & Procedures	8
7	Policy Implementation	9
8	Monitoring & Evaluation	9
9	Review	9
10	Glossary of Terms	9
11	Appendices	

1. Context

1.1 This policy is in place to ensure that the Lee Valley Regional Park Authority ("the LVRPA") complies fully with its legal obligations under the General Data Protection Regulations (GDPR) regarding the handling of the personal data of its customers, suppliers, employees, workers and other third parties.

1.2 This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, Members, website users or any other data subject.

2. Policy Aims

2.1 All employees or partner organisations (suppliers and contractors) who have been permitted access by the LVRPA to personal data must familiarise themselves with the policy and ensure that its terms are fully applied in relation to the handling or "processing" of personal data. It is important that employees understand their obligations under the GDPR data protection principles in respect of the personal information of customers, contractors and staff.

2.2 This policy sets out the minimum standards for compliance with the GDPR and in particular, the Data Protection Principles. All individuals have a right to know who has access to their personal information and for what purpose. By adopting the standards set out in this document we can be assured that our own privacy is respected and we can share this reassurance with everyone we deal with.

2.3 This policy concerns personal data handled by the LVRPA in relation to any person.

Data Protection is monitored by the Information Commissioner's Office, an independent official body. The Commissioner has the power to fine or take legal action against organisations found to be in breach of the GDPR. LVRPA is exposed to potential fines of up to EUR20million (approximately £18million) or 4% of total worldwide annual turnover, whichever is the higher and depending on the breach, for failure to comply with the provisions of the GDPR.

Please contact LVRPA's Data Protection Officer with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

It does not form part of an employee's contract and may be amended at any time. Please check back regularly to obtain the latest copy of this policy.

The LVRPA's Data Protection Officer is:

Beryl Foster,
Lee Valley Regional Park Authority
Myddelton House
Bulls Cross
Enfield
Middlesex
EN2 9HG
T: 01992 709836
E: bfoster@leevalleypark.org.uk

3. Content

3.1 Data Handling

Individuals have rights with regard to how information about them is handled.

LVRPA collects and uses certain types of information about people with whom it deals in order to operate. This includes current, past and prospective employees, suppliers, clients and customers and others with whom we communicate. In addition, we may be occasionally required by law to collect and use such information to comply with government legal compliance and regulatory bodies.

Personal data must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or recorded on other formats - and there are safeguards to ensure this in the GDPR.

3.2 We recognise that the lawful and correct treatment of personal information by LVRPA is important for successful operations and maintaining customer confidence. We therefore ensure that the LVRPA treats personal information lawfully and correctly.

To this end we fully endorse and adhere to the Principles of data protection as set out in the GDPR.

3.3 The Data Protection Principles

Anyone processing data must comply with the following principles.

Personal data shall be:

'Lawfulness, fairness and transparency':

- Processed lawfully, fairly and in a transparent manner;

'Purpose limitation':

- Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
    - (Note: Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89(1)) shall not be considered to be incompatible with the initial purposes);

'Data minimisation'':

- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

'Accuracy':

- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

'Storage limitation':

- Not kept longer than is necessary
    - Personal data must not be kept in a form which permits identification of the data subject for longer than needed for the legitimate business purpose/s for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirement;
    - Personal data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89(1)), subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject;
- **'Integrity and confidentiality':**
  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.

LVRPA is responsible for and must be able to demonstrate compliance with the data protection principles listed above ('**Accountability**').

3.4 **Adherence to the GDPR**
Therefore the LVRPA will, through appropriate management and strict application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of information. This means that, for example, where personal data is being processed on the basis of consent given by the data subject, consent must be clearly and positively given – so silence, pre-ticked boxes or inactivity are not sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate

from those other matters. You will need to evidence consents captured and keep records of all consents so that LVRPA can demonstrate compliance with consent requirements;

- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of the time information is held;
- Ensure that the rights of people about whom information is being held, can be fully exercised under GDPR. This includes:
    - the right to be informed that processing is being undertaken;
    - the right of access to one's personal information;
    - the right to rectify one's data
    - the right to be forgotten or erasure
    - the right to restrict processing
    - The right to data portability (data must be accessible in a machine readable format)
    - the right to object to processing of data
    - The right to not be subject of automated decision making and profiling
- Take appropriate technical and organisational security measures to safeguard personal information. This includes, for example, ensuring that only people who have a need to know and are authorised to use the personal data can access it;
- Ensure that personal data (not already in the public domain) is not placed on LVRPA websites without the consent of the data subject or without specifying any other legal basis at the point of collection
- Ensure that personal information is not transferred outside the EEA without suitable safeguards
- Ensure that suitable safeguards and contracts are in place with third party contractors who may have access to data for the purpose of providing a support service to the LVRPA. This means that you may only share the personal data we hold with third parties, such as our service providers if:
    a) they have a need to know the information for the purposes of providing the contracted services;
    b) sharing the personal data complies with the Privacy Statement provided to the data subject and, if required, the data subject's consent has been obtained;

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
d) the transfer complies with any applicable cross border transfer restrictions; and
e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

3.5 In addition, LVRPA will ensure that:

- A Data Protection Officer is appointed to be responsible for the LVRPA's compliance with Data Protection legislation;
- Everyone managing and handling personal information has received appropriate training and understands that they are contractually responsible for following good Data Protection practice;
- Everyone managing and handling personal information is appropriately supervised and trained to do so;
- Anyone wanting to make enquiries about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are clearly described;
- A regular review and audit is made of the way personal information is managed;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated.

Record keeping:

- Full and accurate records are kept of all our data processing activities. These records should include, at a minimum, the name and contact details of the data controller and the Data Protection Officer, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage solutions, personal data transfers, the personal data retention period and a description of the security measures in place.

3.6 **Subject Access Requests**

In line with the data subject's rights, all individuals have the right to ask whether their personal data is being processed by the LVRPA, where it is being processed and what is being processed.

- The LVRPA will adhere to the data subject's right of access by ensuring that all requests for data are forwarded to the appropriate officer immediately according to internal procedures
- Requests shall be processed within one month of receipt
- Responses shall be provided in machine readable format where received electronically;

- They shall be free unless the request is manifestly unfounded, excessive or repetitive
- The LVRPA may charge for extra copies of the same information
- All response to requests for data will be approved by the Data Protection Officer

3.7 Personal information may be withheld from disclosure if it falls under any of the exemptions described in the GDPR.

Where a request is refused the applicant will be informed, reasons for refusal will be provided and the right to complain to the ICO

4. Responsibilities

4.1 This policy will be overseen primarily by the Data Protection Officer of LVRPA supported by the Information Officer of Vibrant Partnerships, support service provider for LVRPA. All members of staff must take individual responsibility for observing good Data Protection practice.

4.2 Any deliberate breach of this policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Data Protection Officer. You should preserve all evidence relating to the potential personal data breach.

5. Legal Considerations

5.1 This policy is based primarily on the General Data Protection Regulations, but has some degree of overlap with other legislation including the the Data Protection (Processing of Sensitive Personal Data) Order 2000 The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004, Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

6. Relevant Policy & Procedures

6.1 This policy operates in conjunction with LVRPA's following policies, procedures, notices and codes:

- Records Management policies
- IT Usage policy
- CCTV Code of Practice

- Privacy Notice
- Records Retention & Disposal Procedure
- User Systems Access Procedure
- Requests for Personal Data Procedure
- Customer Relationship Management Procedure
- Photography and Videography Procedure
- Data Handling Procedures

7. Policy Implementation

7.1 Data Protection training sessions are held every two months and are compulsory for all employees to attend as part of their induction. To supplement the training employees are encouraged to test their knowledge through online training and tests on the LVRPA intranet.

7.2 The Information Officer will carry out annual audits which include elements of Data Protection and ongoing advice on related areas such as CCTV cameras, records retention and information security.

8. Monitoring & Evaluation

8.1 The policy will be monitored and evaluated on effectiveness periodically through regular audits.

8.2 Audits will be designed to test how effectively the policy can assure compliance with all applicable data privacy laws.

8.3 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

9. Review

9.1 This policy will be reviewed every three years or in the light of new legislation or case law.

10. Glossary of Terms

Term	Definition
GDPR	General Data Protection Regulations
LVRPA	Lee Valley Regional Park Authority
Personal Data	Data that identifies a living individual

Data Subject	An individual whose data we process
Data Controller	In control of the use of personal data
Data Processor	Processes data on LVRPA's behalf
The Trust	Lee Valley Leisure Trust Limited
ICO	Information commissioner's Office
UK Data Protection Bill	Will implement derogations and exemptions from the GDPR