

LEIGHTON LINSLADE TOWN COUNCIL

General Data Protection Inspection Report for Leighton Linslade Town
Council – November 2022

*GDPR Inspection
Report November
2022*

CONTENTS

1.	Introduction.....	2
2.	Identification of Personal Data Held.....	2
3.	Collection of Personal Data.....	3
4.	Record Management.....	7
5.	Information Sharing.....	8
6.	Conclusion.....	8

1. INTRODUCTION

- 1.1 The General Data Protection Regulations (GDPR) came into force on 25th May 2018. GDPR introduced a number of new requirements, including changes to privacy notices, consent and requests to view personal data. The Data Protection Act 2018 has now been enacted.
- 1.2 A site visit was carried out on 9th and 10th November 2022 and this report reviews the existing mechanisms within your organisation for processing personal data and contains recommendations to improve and enhance your compliance with the Data Protection Act 2022.
- 1.3 The Inspection covered 4 parts:
- Identification of what personal data is held;
 - Collection of personal data;
 - Records management;
 - Information sharing.

2. IDENTIFICATION OF PERSONAL DATA HELD

- 2.1 In order to carry out its functions and deliver its services Leighton Linlade Town Council does collect personal data.
- 2.2 The following areas collect personal data within the Town Council:
- Finance & Administration;
 - Councillor information;
 - HR, Payroll, Personnel;
 - Youth services (TACTIC);
 - Cemetery Services;
 - Allotment Services;
 - Civic Functions;
 - Facility Hirers;
 - Venues and facilities for hire;
 - Newsletter;
 - Website and Social Media;
 - Complaints/enquiries;
 - Markets.
- 2.3 All data storage for Leighton Linlade Town Council is located at the White House, Hockliffe Street, Leighton Buzzard LU7 1HD.
- 2.4 The Town Council keeps both electronic and paper based records. These are stored at the White House.

Privacy notices are on all relevant documentation including, where necessary, the facility to obtain consent.

A Data Protection Policy and a Data Breach Procedure was adopted in 2018 by the Town Council but these need to be reviewed.

The Data Retention Policy has been updated and adopted by Council. This includes the deletion, erasure and updating/correcting of information. The Policy now needs to be reviewed to ensure that it continues to be fit for purpose.

All staff are aware of GDPR and it has now become part of the Council culture to consider Data Protection as part of carrying out daily tasks. Regular reminders are sent out and training is provided.

2.5 Biometric data includes technology that identifies employees based on physical characteristics, such as fingerprints, iris colour, or voice recognition. The most common use of biometric data at present is fingerprints (smartphone access) and voice recognition. The Town Council does not collect any biometric information.

2.6 Personal information is updated when up to date personal data is received. The Town Council is aware that personal data needs to be updated regularly and is constantly reviewing its procedures to ensure that data retained is up to date. Each department deals with the updating of personal information based on the way it delivers the service and departmental processes are reviewed.

A process to update Cemetery records regularly to ensure contacts are correct needs to be developed.

Allotment records are updated annually.

Civic lists are updated annually and consent sought where required.

Market information is updated on an ad-hoc basis.

Event information is updated annually.

Booking of venues contact information is retained according to the Retention Policy and updated on an ad-hoc basis.

Email lists are managed through specific software and subscribers have the opportunity to unsubscribe.

The majority of data collection is undertaken electronically and there are processes in place to update and delete information in line with GDPR requirements.

3. COLLECTION OF PERSONAL DATA

3.1 The Town Council continues to collect personal data as identified below

Class of Record	Purpose
Personnel Records	<ul style="list-style-type: none"> To keep a record of all staff employed by the Town Council; Contract requirement;

	<ul style="list-style-type: none"> • Health & Safety; • Insurance; • Legal requirement.
Councillor personal information	<ul style="list-style-type: none"> • To deliver democratic representation as part of the LGA 1972; • To provide open and transparent governance; • Health & Safety; • Insurance
Contractor information	<ul style="list-style-type: none"> • To keep a record of all contractors providing services for and on behalf of the Town Council; • To pay outstanding accounts; • Contract requirement; • Health & Safety; • Insurance; • Legal requirement.
Residents	<ul style="list-style-type: none"> • Service delivery; • Improving, developing and addressing service issues; • Electoral role; • Improving the Town Council.
Businesses	<ul style="list-style-type: none"> • Service delivery; • Improving and investing in the Town
Hirers	<ul style="list-style-type: none"> • Service delivery; • Contract requirement • Health & Safety; • Insurance; • Legal requirement.
Complaints	<ul style="list-style-type: none"> • Service delivery; • Improving, developing and addressing service issues; • Improving the Town Council.
Volunteers	<ul style="list-style-type: none"> • To keep a record of all volunteers providing voluntary services to enable a range of services to be delivered; • Contract requirement; • Health & Safety; • Insurance; • Legal requirement.
Cemetery	<ul style="list-style-type: none"> • Legal requirement to maintain burial records; • Contract requirement with regard to leasing plots;

	<ul style="list-style-type: none"> • Service delivery; • Health & Safety; • Insurance.
Allotments	<ul style="list-style-type: none"> • Legal requirement to maintain allotment register; • Contract requirement with regard to leasing plots; • Service delivery; • Health & Safety; • Insurance.
Markets	<ul style="list-style-type: none"> • Service delivery; • Contract requirement; • Health & Safety; • Risk Assessment; • Insurance; • Legal requirement.
Events	<ul style="list-style-type: none"> • Risk Assessment; • Health & Safety; • Insurance; • Legal requirement.
TACTIC	<ul style="list-style-type: none"> • Service delivery; • Contract requirement • Health & Safety; • Insurance; • Legal requirement.

3.2 The Town Council includes one or more of the lawful basis for collecting information in its privacy notices. These are outlined below:

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides

those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3 The legal basis for collecting the personal information has not altered and is as follows:

Class of Record	Legal Basis
Personnel Records	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation; • Vital Interests.
Councillor personal information	<ul style="list-style-type: none"> • Explicit Consent; • Public Interest; • Contractual necessity; • Compliance with legal obligation.
Contractor information	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation.
Residents	<ul style="list-style-type: none"> • Public Interest; • Compliance with legal obligation; • Explicit Consent.
Businesses	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation;
Hirers	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation; • Explicit Consent.
Complaints	<ul style="list-style-type: none"> • Public Interest; • Compliance with legal obligation; • Explicit Consent.
Cemetery	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation.
Neighbourhood Development Plan	<ul style="list-style-type: none"> • Public Interest; • Explicit Consent.
Allotments	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation; • Explicit consent.
Markets	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation.
Events	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation; • Explicit Consent.
TACTIC	<ul style="list-style-type: none"> • Contractual necessity; • Compliance with legal obligation; • Explicit Consent.

All Privacy Notices contain the legal basis outlining the reason why the Town Council is collecting the information.

Privacy notices are in place for data collection requirements.

An email response privacy notice is included on all emails outlining the Town Council's commitment to Data Protection.

The website includes data protection information, the rights of the individual to access their information and contact information of the ICO.

3.4 Consent, where required, is normally sought and obtained verbally. Consent is recorded where necessary. General enquiries are managed under the Data Protection Act 2018 requirements..

4. RECORD MANAGEMENT

4.1 Records are stored at the Town Council Offices. A range and variety of records are stored, some of which contain sensitive personal information. Council is moving to a Cloud based IT infrastructure so this will reduce the security risk of an in-house server.

4.2 Storage of electronic files are currently held the in-house main server with a Cloud back-up offsite. This is managed by the Council's IT consultant. In-house servers are always going to be more vulnerable to hacking and other attacks. Ensuring that all files are securely backed up on a daily basis will help address any data lost through possible ransom attacks and other virus attacks.

4.3 Access to records are based on the sensitivity of the records being stored. The Council has two restricted drives and a shared drive. It is good practice to protect some sensitive files with passwords to help protect very sensitive information.

4.4 The following electronic access controls are in place:

- Password protected computer access;
- Restricted physical access to the Council Offices;
- Payroll is on a restricted drive which has password protection in place;
- All computers and software access are password protected;
- Sensitive files and folders have restricted access.

- All computers have antivirus protection;
- The IT infrastructure is being transferred to a new Cloud based system provided by a Sector acknowledged service provider;
- Ensure that there continues to be restricted access drives for sensitive information and services.

4.5 The following manual access controls are in place:

- The main Council Office are locked and alarmed when not in use;
- Restricted access to the Offices and storage areas;
- The building has an alarm fitted;
- All offices can be locked when not in use.

4.6 The following manual storage systems are in place:

- Open shelving;
- Secured filing cabinets;
- Unsecured filing cabinets;
- Secured desk drawers;
- Unsecured desk drawers;

4.7 Data retention processes are now being implemented.

- The Data Retention policy has been adopted;
- Records no longer required are disposal of and electronic records are erased as required;
- Personal information is updated on a regular basis depending on the service being delivered;
- Service Level Agreements are GDPR compliant;
- All computers are running on Windows 10.

4.8 Town Council emails are stored on the Cloud in the UK. All staff and Councillor emails are @leightonlinlade-tc.gov.uk.

4.9 The Data Protection audit identified that not all Councillors currently utilise their official .gov.uk emails. **It is strongly recommended** that every Councillor gets into the habit of using their official email addresses as the potential risk of a data breach significantly increases if personal or unofficial email addresses are used. Please see Appendix One of this report for further information.

4.9 The Council uses the Outlook email client for its emails. Each staff member manages their emails differently but they all delete emails that are no longer required and only store emails that are essential for the delivery of council services.

5. INFORMATION SHARING

5.1 The Town Council shares some of its information with various contractors and agencies to enable it to deliver its services and operate efficiently. The sharing of data is outlined in its Data Protection policy and the relevant privacy notices.

5.2 There are data sharing agreements in place for the sharing of personal data with Council agents, suppliers and contractors as well as other data controllers, such as local authorities, community groups, charities and credit reference agencies.

6. CONCLUSION

6.1 The Town Council is currently compliant with the Data Protection Act 2018 and has taken a range of actions to improve its compliance. There will always be opportunities to improve compliance and a number of recommendations are contained in the accompanying Data Protection Audit document.

- 6.2 The Town Council continues to keep GDPR under review on a proactive basis, and has put in place systems to assess compliance in the future, such as carrying out regular data protection audits, Data Privacy Impact Assessments (DPIA) for new projects and regular training for both staff and councillors.
- 6.3 The Council is committed to reviewing its data protection policies on a regular basis and will be reviewing its main Data Protection Policy in the next few months.
- 6.4 The Council's IT provision and storage of electronic data is in the process of transferring to a Cloud hosted system. This will improve basic security of Council data. It is suggested that Council reviews its IT provision every five years to ensure that its IT provision is fit for purpose and is keeping up with technical advances.
- 6.5 The following actions need to be considered over the next twelve months:
- Training for new staff and refresher training for existing staff
 - Training for new Councillors and refresher training for existing Councillors;
 - All Councillors to be encouraged to use only their official council email address for all council related business correspondence;
 - The Data Protection Audit review be considered by the relevant Committee;
 - Council continues to include privacy notices on all relevant documentation and continue to update them as required;
 - That the recommendations in the Data Audit Review be considered and actioned where appropriate;
 - Council should note that any new service delivery will require a Data Protection Impact Assessment (DPIA) to be carried out.