Loddon Town Council

The Library Annexe | Church Plain | Loddon | NR14 6EX

www.loddonpc.org.uk | clerk@loddonpc.org.uk | 01508 522 020

Data Protection Policy

Introduction

The staff and councillors of Loddon Town Council, referred to as LTC hereafter, are committed to adhere to all relevant UK laws, including but not limited to the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, in respect of personal data and the protection of the 'rights and freedoms' of individuals whose personal data LTC is processing.

Policy applicability

This policy applies to all staff and councillors, all of whom have a collective responsibility for the proper processing of the personal data for which LTC is responsible. Any incident or potential data breach is to be reported to the LTC Clerk (see below) in the first instance and without delay. LTC is registered with the Information Commissioner's Office (ICO).

Appointment of the Privacy Manager and external Data Protection Officer

The LTC appointed member of staff who is primarily responsible for all aspects of personal data processing, is the LTC Clerk, who is in effect the privacy manager (PM). The PM is responsible for instigating regular reviews of the relevant documentation, and the maintenance of media used to collect and process personal data, and its eventual return, destruction and/or deletion. The PM is also first point of contact for anyone seeking clarification on any aspect of data protection compliance.

The PM is supported by an external data protection officer (DPO) who is to assist, advise and guide the PM in their role. The DPO is engaged on an as required basis and resourced from LTC funds, subject to prior approval by LTC. Detailed descriptions of the PM and DPO roles are provided in Annex A to this policy.

Policy coverage

This policy applies to the personal data processing functions within LTC including, but not limited to, those performed about its employees, customers, visitors and associated support personnel, suppliers and contractors.

Scope of responsibility

Compliance with data protection legislation is the responsibility of all staff and councillors who process the personal data by or on behalf of LTC. Any misuse or abuse of personal data, whether intentionally or not, will be dealt with by LTC for further action. This may include notifying the ICO. A record of all such incidents is to be recorded in an Incident and Data Breach Register which is to be maintained by the PM.

Third party contractors working with LTC are expected to understand the basic premise of this policy and be subject to a data processing agreement or a non-disclosure agreement (or similar).

Data protection principles

LTC will ensure that the processing of all personal data will be conducted in accordance with the data protection principles shown, in so much that it will be:

- Processed lawfully, fairly and transparently

- Collected for a specified, explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary (and no more)
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security

LTC is to be transparent and fair in all aspects of processing personal data. A privacy statement that explains how LTC manages the personal data of service users, is to be made available on the LTC website in a downloadable form. It is subject to review at intervals of no more than 12 months.

Accountability

LTC is to be fully accountable for the way it processes all personal data and must be able to demonstrate its ability to meet the spirit of data protection legislation at all times. This will be done through the implementation of policies, effective working practices, adhering to codes of conduct and implementing technical and organisational measures including breach notification procedures and incident response plans.

The role of LTC in data protection terms

LTC is a data controller where it determines the purpose and means of processing, and a data processor where it follows the instructions of a data controller – the function of processing will determine LTC's status for any particular operation.

Transparency

Key to the good practice of processing personal data is for LTC to be transparent in its processes and the way it communicates with the people whose data is being processed. As such, LTC is to:

- Publish a website privacy statement that can viewed easily and is downloadable
- Issue Privacy Notices (PN) to specific categories of people when necessary. Each PN is to be prepared in accordance with Articles 13 & 14 of the UK GDPR and set out:
    - What information is collected why it is collected and against which lawful basis
    - The source of the personal data if it did not come directly from the data subject
    - How that information is to be used
    - To whom personal data might be disclosed
    - How data subjects' rights can be exercised

Where the personal data is processed and stored

All personal data that LTC collects or generates in hard copy form is processed, stored and eventually destroyed on its premises. Other (non-paper) based data is gathered and processed by on the local office IT system which it is backed up with a cloud service provider where the servers are based in the EU. Email is processed using a reputable web-based provider. Email and mobile phone contacts are stored on office IT equipment and mobile phones, including those of the councillors. LTC uses appropriate technical and organisational measures to ensure personal data is kept secure.

Lawful bases for processing

LTC will only routinely process your personal data against a lawful basis as described below:

- When it is necessary for the performance of LTC tasks carried out in the public interest and in exercise of the official authority vested in LTC by UK legislation
- To fulfil contractual obligations to including contract preparation
- When processing is necessary for the purposes of our legitimate interests
- To comply with legal obligations
- When processing against a pre-defined purpose for which consent has been sought and recorded prior to that processing commencing.

Change of purpose of processing

From the outset, LTC will state the purpose for which personal data is collected. If this purpose is changed, the affected individuals will be contacted with the relevant information and further appropriate action will be taken if required. Processing of personal data against the new purpose will not commence until either permission has been received or the affected people have been informed.

Processing of children's personal data

LTC is not to process children's personal data as a matter of routine. When it is necessary or unavoidable, written consent must be sought from the relevant child's parents/ guardian before processing takes place. For the purposes of this policy, this clause only effects children who have not reached their 13th birthday at the time of processing.

Training

All LTC staff who routinely handle personal data as part of their role are to undertake regular training (at least annually) to instruct or remind them of the basics of data protection. The LTC PM and are to receive more thorough training as befits their roles. The training can be conducted by any competent staff member with the requisite experience and knowledge, on-line or delivered by an external trainer if necessary.

Third-Party support workers (contractors)

Those that support LTC's operations but are not employed, such as contractors, are to be briefed on their responsibilities regarding the handling of personal data. The extent of such briefings will depend on each role so is not specified in detail in this policy, however, the expectation is that as a minimum, contractors:

- Are made aware of this policy and who the PM is
- Are made aware of any specific role conditions
- Delete any LTC related personal data (other than that used for domestic purposes), prior to the end of their contracts
- Are made aware of the need for reporting incidents and possible data breaches and how they can do so
- Be issued with a privacy notice that explains how LTC processes their personal data

Security of data

LTC operates a 'need to know' principle but will always try to get the right balance between ensuring the privacy of the individual and being able to offer an effective and efficient service to service users.

Whilst the overall responsibility for the implementation of data protection policies and procedures lies with the PM, all staff and councillors are responsible for the personal data they process. This includes, but is not limited to, keeping information secure when not in use and keeping documentation out of sight of those that have no reason to view it.

IT Security

LTC uses a trusted third-party IT service provider to ensure, in so far it is possible, that all data processed meets the requirements set out in data protection legislation, in so far that it is possible. The office IT system is to be configured to ensure the appropriate level of confidentiality, availability and integrity of the personal data being processed on-site.

Due diligence is applied to ensure that the service offering is appropriate to the needs of the business and that the staff of the third-party understands their responsibilities in terms of respecting the confidential nature of the personal data it has access to. The engaged IT service provider is to be subject to a data processing agreement as required by Article 28 of the UK GDPR.

Physical Security

The application of appropriate physical measures in an organisation is intricate to the responsible processing of information, particularly personal data. LTC adopts a layered approach to physical

security such that there is no single point of failure. In brief, physical security is maintained through:

- A combination of on-site employees with dedicated security duties
- The use of combination coded locks for building access when doors are unlocked during office
- Use of lockable filing cabinets for storage of hard copy information and other storage media where the keys are assigned to nominated individuals
- Lockable doors that remain locked by default but opened during office hours
- Controlled access to the master keys for all lockable doors
- A record of staff, Councillors and contractors that have access to the master keys

Use of on-site CCTV

LTC has a legitimate interest to deploy CCTV systems for the detection and prevention of crime. The routine operation of the CCTV system is to be managed by the PM in accordance with the LTC CCTV operation policy.

Where CCTV is deployed, there is to be adequate signage to ensure anyone visiting the site is made aware that CCTV is in operation. Unless circumstances justify, images are not to be retained any longer than 60 days.

Disclosure of personal data

The guiding principle of LTC is that personal data is not to be disclosed to third parties, which includes family members, friends and in some circumstances, the police, unless previously authorised or agreed to by the affected individual. Such authorisation or agreement must be demonstrable and normally involves:

- The prior signing of a confidentiality agreement or Non-Disclosure Agreements
- Court order

It follows that all staff and councillors should exercise caution when asked to disclose personal data held by LTC to a third party. Any such requests must be supported by appropriate evidence that states its purpose and should be retained or recorded. Other than established or regular requests, guidance must be sought from the PM before disclosure. Exceptions to this might be when someone discloses information acting in someone's vital interests; this is normally a 'life and death' situation.

If, subsequently, the disclosure of personal data was deemed to be inappropriate, then this is to be reported to the PM and recorded in the Incident and Data Breach Register. The PM is then to decide on further action as required.

Retention and disposal of data

LTC is to maintain a Retention Schedule and to adopt internal measures to ensure staff and councillors do not retain personal data in a form that permits identification for longer than is needed or justified in law. Personal data may be stored beyond the schedule, for the purpose of maintaining records and statistics on the grounds of legitimate interest. In all cases the appropriate technical and procedural measures are to be taken to safeguard the rights and freedoms of the affected individuals.

Disposal and destruction of personal data will be conducted under controlled conditions under the guidance of the PM and in accordance with LTC's internal security procedures.

Retention of personal data after the lawful condition for processing has ended

Regardless of the source of personal data held by LTC, once it is no longer needed or no lawful justification exists to retain it, the personal data is to be reduced, deleted or destroyed in accordance with this policy or the schedule set out in service user privacy notices and/or the website privacy statement, within 3 months.

End of staff and councillor tenure

At the end of a staff member or councillor's tenure of office at LTC, they are to delete or destroy all LTC related personal data in their possession, less that which has been made manifestly available

in the public domain. Upon departure from LTC, they are to make a written declaration to that effect and to commit to appropriate action to delete or destroy information, without delay, in the event that they uncover continued possession of such material.

Contact details of people obtained during the course of LTC related activity may be retained by individuals, where its intended use is for purely personal or household activity.

Incident and data breach reporting

LTC staff are to be briefed that the misuse of personal data, whether intentional or otherwise, can have serious consequences for LTC's reputation. Any incident, that might expose someone (regardless of who) in such a way that their rights and freedoms are impacted, is to be reported to the PM. Subsequent action will be determined by the PM based on the severity of the incident. The PM is to seek the advice and guidance of the external DPO when necessary.

In all instances, incidents are to be recorded in a dedicated register. When appropriate, they are to be registered as a data breach and reported to the ICO within 72 hours of the data breach being established, by the PM.

The LTC website

LTC maintains a website as a source of information primarily for the benefit of local residents. If the website uses cookies (or similar technologies) to enhance user experience and to collect analytical data, then user consent must be sought before non-essential cookies are 'dropped'. No attempt must be made to identify the individuals, via technical means or otherwise, that visit the website, unless there is a legal requirement to do so.

Individuals' (Data Subjects') rights

The UK GDPR puts much greater emphasis on transparency of processing and accountability by all parties involved in handling of personal data. It also extends the rights of individuals (referred to as "data subjects") in respect of their personal data. It should be noted that these are limited and do not apply in all situations. These are shown below:

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights related to automated decision making and profiling.

LTC will ensure that individuals may exercise these rights including the handling of Data Subject Access Requests (DSAR) and complaints relating to the processing of an individual's personal data. Before responding to requests, LTC is to verify a requesters/enquirer's identity before responding fully. This typically involves requesting the requester for proof of ID or other material that, in context, enables LTC to confirm the necessary identity.

Data transfers

LTC does not ordinarily transfer personal data outside the UK and does not use services (such as back-ups) that rely on data processing outside the UK. If the situation arises that data might be transferred outside the EU, the PM will assess the impact of such processing based on the destination client and country.

Information asset register/ data inventory

LTC is to maintain a high-level data inventory that maps the flow of personal data into and out of the organisation. This is to be used to identify areas of security vulnerability, whether paper or IT related as well as the need for specific to audience privacy notices, if appropriate.

Data Protection Documentation

The overall approach to the creation and maintenance of the suite of documents, that form LTC's privacy framework, is to take account of the associated risks, as defined on LTC's risk register. LTC is to maintain such a privacy framework such that it can demonstrate the processing of personal data in a responsible and lawful way. The key documents to be maintained are as follows:

- Data Protection Policy – primarily for the benefit of all staff and councillors
- Privacy Statement – to be made available on the website in a downloadable form
- Record of data processing activity – high level only
- Information security policy relating to the wider use of the IT support system
- Incident and Data Breach Register – to be controlled by the PM
- CCTV Usage Policy

In addition, privacy notices are to be prepared, when appropriate, for specific categories of people.

Policy reviews and updates

Data protection related documents are to be reviewed annually as part of LTC's overall audit programme. Such activity may happen more frequently as advised by the PM, in particular to take account of:

- Incidents and data breaches that might require a review of existing procedures
- When compelled to do so by the ICO
- Changes to UK legislation

Document owner, approval and availability

The LTC Clerk is the owner of this policy document and is responsible for ensuring it is reviewed in line with all requirements set out above. The document is subject to version control and approval by LTC.

This policy was adopted by Loddon Town Council at its meeting held on the 12 April 2023.

Signed: Dated:

Date for next review: April 2026 (reviewed every three years).

Annex A

Roles of the Privacy Manager (PM) and the External Data Protection Officer

LTC Privacy Manager (PM)

The PM is appointed by LTC management to provide first line support to its staff on data protection law, its compliance and the implementation of related policies and procedures. The default appointee is the LTC Clerk.

Specific tasks

In particular, the PM is to:

- Attend such training, either in person or on-line, to ensure they have the requisite level of data protection knowledge to be effective in the role
- Provide first line support to LTC staff regarding data protection matters and to assess incidents in accordance with LTC's incident reporting procedures
- Liaise with the DPO at the point when the PM needs additional guidance or when there is a legal necessity for the DPO to intervene
- Provide the DPO with access to LTC staff and councillors for the purposes of awareness briefing, reviewing extant processes and investigating incidents
- Provide the DPO with access to personal data and processing operations for the purposes of investigating incidents
- Provide a suitable workplace for the DPO and any related staff when visiting LTC's premises and access to virtual meeting facilities when required
- Maintain LTC's annual registration with the ICO

External Data Protection Officer (DPO)

Based on the tasks described in the UK GDPR, the DPO shall:

- Advise LTC on matters relating to the processing of personal data, including the investigation of potential data breaches and the implementation of Freedom of Information (FOI) requests
- Routinely monitor how LTC meets the legislation through the implementation of policies, and assignment of responsibilities, awareness briefings, training, and audits
- Provide advice regarding the need for, and the processing of, Data Protection Impact Assessments (DPIA)
- Cooperate with the Information Commissioner's Office (ICO) and to be LTC's point of contact for the handling of data breaches and other appropriate matters
- Be available to all LTC staff and councillors who wish to raise issues relating to the processing of their personal data and to exercise their rights.

These tasks shall take due regard of the risk associated with the processing operations, considering the nature, scope, context, and purposes of processing by LTC. Accordingly, the DPO is bound by confidentiality concerning the performance of the duties and is, in any event, subject to the conditions set out in the UK GDPR for data processors.