SHERINGHAM TOWN COUNCIL – DATA PROTECTION POLICY (DPP)

Introduction

Sheringham Town Council (STC) is committed to adhering to all relevant UK data protection legislation, 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 information STC collects and processes in its role as a local public authority (PA).

Policy applicability

This policy applies to all STC councillors and staff (full time and part time) as well as contractors, all of whom have a collective responsibility for the proper processing of the personal data for which STC is responsible. Any incident or potential data breach is to be reported to the internal privacy manager DM in the first instance and without undue delay.

Appointment of the data manager (DM)

The STC data manager ("DM"), is responsible for all aspects of personal and non-personal data being processed for STC. This includes annual reviews, and the regular maintenance of media used to collect and process personal data, and its eventual return, destruction and/or deletion. The DM is also first point of contact for anyone seeking clarification on any aspect of data protection compliance. The town clerk is the default DM unless STC choose another appointee.

With respect to personal data processing, the DM may be supported by an external data protection specialist ("DP Support"). The roles and responsibilities of the DM and DP Support are set out in Annex A.

Scope of responsibility

Compliance with data protection legislation is the responsibility of all councillors, the staff of STC and contractors who process the personal data on behalf of STC. Any misuse or abuse of personal data, whether intentionally or not, will be dealt with by STC for further action. This may include notifying the Information Commissioner's Office (ICO) or law enforcement bodies. A record of all such incidents is to be registered in an Incident and Data Breach Register which is to be maintained by, and under the control of, the DM.

Third party contractors working with STC are expected to understand the basic premise of this policy and will, when necessary, be issued with a Privacy Notice (PN). They will also enter into a data processing agreement if their role includes processing personal data on behalf of STC and where their contract does not include the relevant clauses found in Article 28 of the UK GDPR.

Data protection principles

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

- Processed lawfully, fairly and transparently
- Collected for a specified, explicit and legitimate purposes
- 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

Accountability

STC is to be fully accountable for the way it processes all personal data and must be able to demonstrate its ability to meet its legal requirements as set out in the relevant legislation. This will be done through the implementation of policies, effective working practices, adhering to any relevant codes of conduct and implementing technical and organisational measures that include personal data breach notification and incident response procedures.

Lawful conditions for processing

STC collects personal data for a variety of reasons and the lawful condition for doing so will vary accordingly. The principle lawful basis that STC will engage is *"where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"* (Article 6.1(e) UK GDPR).

This does not exclude relying on the other lawful reasons to process personal data and STC will also do so where circumstances require, in particular:

- With consent that is established prior to any processing
- To meet its contractual obligations
- To comply with its legal obligations
- When acting in the vital interests of an individual
- In pursuit of STC's stated legitimate interests, where it is assessed that its actions do not over-ride the rights and freedoms of the affected individual(s)

Transparency

STC is to be transparent in its processes and the way it communicates with the people whose personal data is being managed. Accordingly, STC is to publish and maintain a general website privacy notice (PN). This must be easily viewable and downloadable as a pdf document for ease of access. It is not necessary for STC to confirm that the PN has been read. In addition, STC is to make available separate PNs specific to the recipient when appropriate, in particular for employees/ contractors and suppliers among others.

PNs are to set out:

- What information is collected why, and against which lawful basis
- The source of the personal data if it did not come directly from the data subject

- Details on how people can contact the privacy manager and the ICO
- How the information is to be used and for how long
- To whom personal data might be disclosed
- How people can exercise their data protection
- Where the personal data is processed and stored

The council's server is backed up in the UK and the EU.

Use of consent

Consent means any freely given, specific, informed, and unambiguous indication of an individual's wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Further details on how consent is to be managed, is included in Annex B.

Change of purpose of processing

From the outset, STC will state all purposes for which personal data is collected. If a purpose changes significantly, the affected individuals will be contacted with the relevant information and further appropriate action will be taken as required. The processing of personal data against the new purpose will not commence until either permission has been received (if it is required) or the affected people have been informed.

Training

All STC staff who routinely handle personal data as part of their role are to undertake regular training (at least annually) to ensure they understand their data protection obligations appropriate to their responsibilities. All councillors are expected to undertake UK GDPR awareness training upon appointment, as well as continuity training annually. The scope and depth of all training is to be proportionate to the various roles and is to be designed and delivered by a data protection specialist.

Third-Party support workers (contractors)

Third party organisations that support STC operations but are not employed by STC such as contractors, consultants and experts (for fundraising) are to be briefed on their responsibilities regarding the handling of personal data. The content of such briefings will depend on the role, but the expectation is that, as a minimum, contractors:

- Are to be made aware of this policy and the identity of the DM
- Are to be made aware of any immediate role requirements such as deleting any personal data stored on electronically or in paper form, upon completion of their contract
- Are to delete any STC related personal data other than that used for domestic purposes, prior to the end of their contract
- Are to be made aware of the need for reporting incidents and potential personal data breaches and how this can be done
- Are to be issued with or given access to the STC general privacy notice or given access to a contractor's specific privacy notice when required

Security of data

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

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

IT Security

The DM is responsible for the first line maintenance of the IT system and the application of appropriate security measures to be set out in the STC Information Security (InfoSec) Policy.

Where STC uses third-party IT service support services, it is to ensure, in so far it is possible, that all data being processed is proportionate for the purpose and that the IT support organisation enables the appropriate level of confidentiality, availability and integrity of the personal data processed on-site.

Due diligence is applied to ensure that the service offering is appropriate to the needs of the council and that the IT service support company understands their responsibilities in terms of respecting the confidential nature of the personal data it has access to. The IT service support organisation is subject to a data processing agreement as required by Article 28 of the UK GDPR.

Working from home

All STC councillors and staff will work from home ("WFH") at some stage so the application of appropriate physical measures is necessary for the responsible processing of personal data. These measures are included in specific WFH guidance to be made available in the InfoSec policy which is also to incorporate use of personal device directives.

STC adopts a layered approach to physical security such that there is no single point of failure. In brief, home security will need to be managed locally and such measures taken may include the following the use of lockable filing cabinets for storage of hard copy information and other storage media where the rooms afford a reasonable degree of privacy from co-inhabitants.

Misuse of personal data

All staff are to be briefed that the misuse of personal data, whether intentional or otherwise, can have serious consequences for the council's reputation and impact operational effectiveness. 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 DM. Subsequent action will be determined by the DM based on the severity of the incident. The DM is to seek the advice and guidance from DP Support, as required.

Disclosure of data

The guiding principle of STC 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 signing of a confidentiality agreement or Non-Disclosure Agreements
- A court order

It follows that councillors, staff and contractors should exercise extreme caution when asked to disclose personal data held by STC, 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 DM before disclosure. Exceptions to this might be when someone must disclose information to act in an individual's vital interests. This is normally a 'life and death' situation where the affected individual is not in a position to give consent for their personal data to be disclosed.

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

Retention and disposal of data

STC is to maintain a Retention Schedule and to adopt measures such that staff 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 after it has been reviewed and reduced to a minimum, for the purpose of maintaining records and statistics. 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 as set out by the DM and in accordance with STC InfoSec policy.

Regardless of the source of personal data held by STC, 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 the Retention Schedule within 3 months of the retention period ending.

Incident and data breach reporting

STC councillors and staff are to be briefed that the misuse of personal data, whether intentional or otherwise, can have serious consequences for STC's reputation and operational effectiveness. 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 DM. Subsequent action will be determined by the DM based on the severity of the incident. The DM is to seek the advice and guidance of the DP Support (if appointed), when necessary.

In all instances, incidents and personal data breaches are to be recorded in a dedicated register maintained by the DM. If a data breach is deemed serious enough, it is to be reported to the ICO within 72 hours of the data breach being established, regardless of weekends and/or seasonal holidays.

STC website

STC maintains a website for publicity purposes and as a source of information for the local community. The websites use cookies to enhance user experience and to collect analytical data of the web browsers used to view the website. User consent must be sought before non-essential cookies are run. 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.

Individual data subject rights (DSR) and complaints

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. Collectively, they are referred to as data subject rights (DSR). Notification these rights, and the opportunity to complain, are to be published on all privacy notices. It should be noted that the DSRs 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.

STC will ensure that individuals may exercise these rights including the handling of Subject Access Requests (SAR) and complaints relating to the processing of an individual's personal data. A separate procedures document is to be maintained to facilitate the administration of dealing with all 'rights' requests.

The DM is to review and handle all requests in the first instance and ensure that these are dealt with within the required timelines and with the appropriate responses.

In those instances that inaccurate information about an individual needs to be updated and where the original information was provided to third-parties, those organisations are to be notified of the changes, unless this is deemed to involve a disproportional effort. The same applies for personal data that has been erased.

Individuals that complain, as opposed to exercising their rights, are to have their complaints reviewed by the DM in the first instance. All complaints are to be responded to as appropriate unless the complainant is deemed to be unjustifiably persistent or vexatious in nature. Under these circumstances, STC may choose to provide a final response indicating

that no further correspondence will be entered into for a pre-determined length of time, e.g. 12 months, and that the complainant should take their issues to the ICO or seek a judicial review.

Data transfers

STC 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 EEA, the DM will assess the impact of such processing and seek further advice as necessary.

Information asset register/ data inventory

STC is to maintain a high-level data inventory that identifies the flow of personal data into and out of the organisation. This is primarily used to demonstrate good data management and also to identify areas of points of security related vulnerabilities.

The above is based on an initial assessment of risk to individuals associated with the processing of their personal data. STC is to conduct risk assessments annually and in response to an incident or data breach, whichever comes first, and instigate appropriate actions to reduce the possibility of mal-practice or non-conformance with this policy.

Data protection documentation

STC will maintain sufficient documentation with respect to the processing of personal data, to be able to demonstrate that it is following structured processes in a responsible and lawful way. All documentation is to be subject to version control and STC approval mechanisms. The documentation is to cover all activities that involve the processing of personal data including, but not restricted to:

- Data Protection Policy (DPP) – an internal document available to all staff and contractors
- Privacy Notices – a general notice to be made available on each website (and downloadable) and specific to category notices, to be issued when required
- Record of data processing activity/ data flows – high level only
- Personal data retention policy and schedule
- Information security (InfoSec) policy
- Incident and Data Breach Register – to be managed by the DM
- The deployment of CCTV and image disclosure
- Data subject rights
- Working from home (WFH) and use of own devices, to be included as an annex to the InfoSec policy

Policy reviews and updates

Data protection related documentation is be reviewed annually as part of the overall STC audit programme. Such activity may happen more frequently as advised by the DM, 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
- When a policy is still being developed
- Changes to the legislation

Document owner, approval and availability

The DM 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 STC.

The document and any later versions are to be made available to all staff and contractors, such that they might reasonably have access to it in the normal course of their duties.

V1.0

May 2025

Annexes:

A. Roles of the data manager and the data protection specialist support
B. Use of Consent

Annex A

Roles of the data manager and the data protection specialist support

STC Data Manager (DM)

The DM is appointed by STC to provide first line support to STC staff on data protection law, its compliance and the implementation of related policies and procedures.

Specific tasks

In particular, the DM 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 STC staff regarding data protection matters and to assess incidents in accordance with STC's incident reporting procedures
- Liaise with the DP Support at the point when the DM needs additional guidance or when there is a legal necessity for the DP Support to intervene
- Provide the DP Support with access to STC staff for the purposes of awareness briefing, reviewing extant processes and investigating incidents
- Provide the DP Support with access to personal data and processing operations for the purposes of investigating incidents

Data protection specialist support ("DP Support")

Based on the tasks described in the UK GDPR, DP Support shall:

- Advise STC on all matters relating to the processing of personal data, including the investigation of potential data breaches
- Routinely monitor how STC meets the legislation through its 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 be STC's point of contact for the reporting of data breaches and other appropriate matters

These tasks shall take due regard of the risk associated with the processing operations, considering the nature, scope, context, and purposes of processing by STC. Accordingly, the DP Support is to be bound by confidentiality concerning the performance of their duties and is, in any event, subject to the conditions set out in the UK GDPR and the Data Protection Act 2018.

Annex B

Use of consent

Any requests for consent must be in a form of words to ensure consent would be valid. Additional information is to be provided at the time consent is being requested that will enable the consenting party to have access to the STC website privacy notice.

If consent is indicated only verbally, then a record of this event is to be made including the date on which it was received and the manner it was given. The proper maintenance of such records is necessary to enable STC to be accountable for its actions and to be able to demonstrate that consent was given.

If consent to a particular purpose has not been received, STC is to take it that consent has not been given and the relevant processing activity will not take place.

When explicit consent is relied upon for the processing of sensitive (special category) data, STC is to obtain a signed declaration (or equivalent) from the individual before the processing activity commences.

In all instances, if consent is withdrawn, STC will cease processing the personal data that relates to the specified purpose and record the event.

Document history

Version	Date	Reason for / summary of changes	Author
0.1	05/03/2025	Initial draft	CJIS
0.2	09/04/2025	Updates as per meeting with the clerk	CJIS
0.3	13/05/2025	Updates as per meeting with the clerk, including changes to consent (creation of Annex B), expanding the training section, confirming regions where processing is taking place	CJIS
1.0	15/05/2025	Formatting for submission to Full Council for adoption	MB