Date adopted: March 2023
Review date: March 2025
Ratified: Full Council meeting: 28th March 2023

GDPR POLICY

1. Purpose of the policy and background to the General Data Protection

Sheringham Town Council's General Data Protection Regulation policy is based on The General Data Protection Regulation (GDPR) which took effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by.

For the GDPR and the new data protection legislation, the definition of public authorities is the same as that used in the Freedom of Information Act 2000 (which includes local councils and a parish meeting constituted under s. 13 of the Local Government Act 1972) Please note: The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

The council, as data controller, remains responsible for compliance with the data protection legislation including the GDPR. All councillors, staff, committees, sub-committees, co-opted committee members and volunteers are expected to apply data protection legislation in their work. The Clerk, as Data Protection Information Officer, should have access to full council and relevant staff, committees and sub-committees. STC includes data protection roles in all of its committee and task and finish group remits.

The Clerk or Deputy Clerk in their absence fills the role of Data Protection Information Officer and is responsible for advising the Council as to how it should act, it's legal responsibilities and the appropriate processes required in order to comply with GDPR regulations.

2. Information Commissioners Office Registration

The Council does not need to be registered with the ICO but it must pay the annual fee. Individual Councillors will include the council email privacy notice on their email correspondence. If they act as representatives for members of their ward rather than follow Sheringham Town Council Communication policy – requests for information, support etc, they are seen to be acting as an individual Data Controller and must complete their own registration. In the event of a Councillor representing an elector then they must be aware they are working beyond the Sheringham Town Council ICO registration.

3. The Underlying Principles of GDPR and STC GDPR Policy

STC GDPR policy places a great emphasis on transparency, openness and the documents the Council needs to keep in order to show that STC is complying with the legislation. This is incorporated within the idea of "accountability". The GDPR has a number of underlying principles. These include that personal data:

- Must be processed lawfully, fairly and transparently.
- Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
- Should be adequate, relevant and limited (Only the minimum amount of data should be kept)
- Must be accurate and where necessary kept up to date.
- Should not be stored for longer than is necessary, and that storage is safe and secure.
- Should be processed in a manner that ensures appropriate security and protection.

- This policy explains
  - The duties of STC under GDPR and the responsibilities of the council.
  - Identifies the means by which the council will meet its obligations.
  - Identifies the necessary GDPR roles
  - How STC will minimise risk

- GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned.

Transparency - This policy will be displayed on the council website and made available in hard copy if requested.

4. Sheringham Town Council's Lawful basis for processing data

The GDPR sets out six lawful bases for processing data. Unless an exemption applies, at least one of these will apply in all cases. It is possible for more than one to apply at the same time. STC will only process data where such a lawful basis exists and for only for that basis on which consent is given. The six lawful bases for processing personal data under the GDPR and therefore STC policy are:

4.1 Consent - A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action.

4.2 Legitimate interests - This involves a balancing test between the controller's (or a third party's) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests. Please note, councils and parish meetings are public authorities and under the GDPR public authorities cannot rely on legitimate interests as a legal basis for processing personal data.

4.3 Contractual necessity - Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

4.4 Compliance with legal obligation - Personal data may be processed if the controller is legally required to perform such processing, for example complying with the requirements of legislation.

4.5 Vital Interests - Personal data may be processed to protect the 'vital interests' of the data subject. For example: In a life or death situation, it is permissible to use a person's medical or emergency contact information without their consent.

4.6 Public Interest - Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

5. Sheringham Town Council's Lawful basis for processing 'sensitive personal data'

Sensitive personal data, which the GDPR refers to as 'special category data', means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, and sexual life. The GDPR adds the following new additional categories: genetic data, biometric data and sexual orientation. To process sensitive personal data one of the following should apply – however please note that:

- More than one of the criteria below can apply at the same time.
- Data controllers need to establish a lawful basis for processing any personal data (see previous paragraph) and, if they are processing sensitive personal data they must also establish that at least one of the criteria below applies:
  i. Explicit consent of the data subject has been obtained (which can be withdrawn).
  ii. Employment Law – if necessary for employment law or social security or social protection.
  iii. Vital Interests – In a life-or-death situation where the data subject is incapable of giving consent.
  iv. Charities, religious organisations and not for profit organisations – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors. Please note councils and parish meetings cannot rely on (iv) as a lawful basis for processing personal sensitive data.
  v. Data made public by the data subject – the data must have been made public 'manifestly'.
  vi. Legal Claims – where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.
  vii. Reasons of substantial public interest – where proportionate to the aim pursued and the rights of individuals are protected.

viii. Medical Diagnosis or treatment – where necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.

ix. Public Health – where necessary for reasons of public health e.g., safety of medical products.

x. Historical, Statistical or scientific purposes – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

In a council context, the most relevant lawful basis for processing under Special Category Data are likely to be (i), (ii) and (vii), namely: Explicit consent from a person; or Employment law (for staff)

6. Roles under GDPR

Under the GDPR a parish or town council is not a public authority and as a result does not need to appoint a Data Protection Officer. For further information from the ICO see their link; DPOs in our Guide to the GDPR.

Regardless that STC is not obliged to appoint a DPO, STC is still subject to data protection legislation and the Council must ensure that the Council has sufficient staff and resources to discharge the Council's obligations under the GDPR.

7. The Council is the Data Controller. The Data controller is responsible for

- Undertaking an information audit annually,
- Determining the purposes for processing personal data.
- Determining the manner of processing personal data.
- The evaluation of the risk (medium to high risk) from holding and processing personal data and the inclusion of GDPR in the Risk Management Policy and annual audit.

This will be completed through the Finance & Governance Committee and recommendations made to full council.

8. Data Information Officer (DIO)

The Clerk or Deputy Clerk (in the Clerk's absence) is the DIO. The Clerk is responsible for ensuring the completion of an annual information audit and to manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. The clerk is responsible for the minimising of the risk by:

- Undertaking the annual information audit
- Issuing privacy statements
- Obtaining consents where necessary to hold and process personal data
- Initiating and maintaining Data Privacy Impact Assessments (an audit of potential data protection risks)
- Minimising who holds data protected information
- Ensuring the Council undertakes training for councillors, co-opted members, Officers and employees.
- Informing the Council and, where appropriate, the ICO of Data Breaches
- Investigating breaches of personal data and reporting outcomes

9. Individual Councillors, role holders and co-opted committee members and staff members

GDPR requires continued care by everyone within the council (Councillors, volunteers and Staff) in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine from the ICO for the breach itself and also to compensate the individual(s) who could be adversely affected.

All individual employees, volunteers, Councillors and co-opted committee members are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council and must inform the DIO of any breaches of personal data as soon as they become evident.

10. Information Audit

The DIO must undertake an Annual Information Audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy.

The information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Council undertakes a new activity. The Annual information audit review should be conducted ahead of the review of this GDPR Policy and the reviews and recommendations to Full Council by the Policy and Process Committee should be minuted.

11. CCTV in council buildings.

STC has CCTV in place to try to protect the security of buildings. Signage is in place which notifies visitors that they are being recorded and all the purposes the data is collected for. 'CCTV is in operation here in order to protect STC property, staff, Councillors and visitors. It may be used as part of criminal proceedings.'

12. Contracts with suppliers and partners

STC requires that all contracts where a company or other organisation supplies goods and services to the council and processes personal data (companies providing payroll services, CCTV or IT support, etc.) must be in writing and must contain a prescribed list of provisions describing how the data is processed.

The following provisions should be included in STC contracts:

a) Processors must process data only on the instructions of the data controller.
b) People authorised to access data are subject to confidentiality.
c) Ensure security of processing.
d) Processors must assist the controller in complying with data subjects' rights (where possible).
e) Processors must assist the controller with regard to security measures, breach reporting and DPIAs.

SUBJECT ACCESS REQUEST POLICY AND PROCESS:

SAR Policy:

Individuals are entitled to place a Subject Access Request (SAR) with Sheringham Town Council to ascertain what personal information about them is held by STC. Through the privacy statements on the website and sent to STC contacts, STC will inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (a dedicated email address).

The Data Information Officer (DIO) for STC – the Clerk (or Deputy in the Clerk's absence) will be responsible for ensuring compliance with the SAR. A data processor on receipt of a SAR for information on data for which they are not the data controller will inform the data controller immediately of the SAR. Under GDPR, the time limit to comply with a SAR is one month and all SARs are free of charge.

STC GDPR Processes identify how subject data is to be handled, stored and deleted. As a result, subject data information will only be stored electronically in pre-determined folders or in the enquiry folders as hard copy. All changes to data processing will be recorded in STC data log. This enables the staff to search all information held and be confident that a SAR can identify where all of a subject's data is being held in STC data processing activities and to transfer this information where necessary.

Staff, Cllrs and Role holders will not transfer subject's personal data via a memory stick, CD or memory card as part of their council activities. Cllrs should be aware they will be asked to show where they hold subjects' personal data on their personal correspondence where relevant. Councillors are therefore advised to complete the same monthly enquiries deletion process as the office in their own systems.

All personal information which needs to be retained should be passed to the STC office and recorded on the relevant database as per the Sheringham Town Council Communications Policy.

Individuals have the right to have incorrect information rectified, erasure and restriction of processing. The Data Controller will determine if it is appropriate for rectification and restriction of processing. With regard to erasure the Data Information Officer will consider whether there is a legal purpose, which prevents deletion of the subject's data. The individual will be informed of this legal purpose in the event of a refusal to rectify, erase or restrict information.

SAR Process:

A SAR will be responded to by the DIO using the response process. Upon receipt of a SAR all Information Processors (Clerk, Officers, Councillors) must:

1. forward it immediately to the Data Information Officer (DIO)(The Clerk or Deputy Clerk in their absence)
2. correctly identify whether a request has been made under the Data Protection legislation
3. under the guidance and request of the DIO a member of staff, and as appropriate, Councillor or role holder who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive search of the records to which they have access.
4. Ensure all the personal data that has been requested be provided unless an exemption can be applied.
5. respond within one calendar month after accepting the request as valid.
6. Ensure requests be undertaken free of charge to the requestor unless the legislation permits reasonable fees to be charged.
7. ensure that the staff they manage are aware of and follow this guidance.
8. Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint.

STC Process upon receipt of a SAR

1. Notify the DIO upon receipt of a request.

2. The DIO must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. The DIO should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity.

The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence / Shotgun Certificate
- EEA National Identity Card
- Full UK Paper Driving Licence
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*
- State/Local Authority Educational Grant Document*
- HMRC Tax Notification Document
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company+
- Judiciary Document such as a Notice of Hearing, Summons or Court Order
- Utility bill for supply of gas, electric, water or telephone landline+
- Most recent Mortgage Statement
- Most recent council Tax Bill/Demand or Statement
- Tenancy Agreement
- Building Society Passbook which shows a transaction in the last 3 months and your address

3. STC will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc.

4. STC must not withhold personal data because it is believed it will be misunderstood; instead, the Council should provide an explanation with the personal data. STC must provide the personal data in an "intelligible form", which includes explaining any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees

or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on STC premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear on forms and on the council website

6. A database is maintained allowing the Council to report on the volume of requests and compliance against the statutory timescale.

7. When responding to a complaint, STC must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

Responding to a SAR - Sample letters

1. All letters must include the following information:

a) the purposes of the processing.
b) the categories of personal data concerned.
c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules (1) or EU model clauses (2).
d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.
e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
f) the right to lodge a complaint with the Information Commissioners Office (ICO).
g) if the data has not been collected from the data subject: the source of such data.
h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (STC does not currently process information in this way.

(1) Binding Corporate Rules is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations headquarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

(2) EU model clauses are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

2. Replying to a subject access request providing the requested personal data - Sample letter

[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

3. Release of part of the personal data, when the remainder is covered by an exemption – Sample letter

[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. To answer your request, we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose [some/most] of the personal data you requested. [If any personal data has been removed] We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you.

You will notice that [if there are gaps in the document] parts of the document(s) have been blacked out. [OR if there are fewer documents enclose] I have not enclosed all of the personal data you requested. This is because [explain why it is exempt].

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

4. Replying to a SAR explaining why you cannot provide any of the requested personal data – Sample letter

[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject].

I regret that we cannot provide the personal data you requested. This is because [explanation where appropriate].

[Examples include where one of the exemptions under the data protection legislation applies. For example, the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer (Advise to be obtained from NALC)will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely

(a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

5. Responding to a SAR

(a) Respond to a SAR within one month after receipt of the request.

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month.

(ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing

(vi) the right to lodge a complaint with the Information Commissioners Office (ICO)

(vii) if the data has not been collected from the data subject: the source of such data;

(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Provide a copy of the personal data undergoing processing.

SECURITY INCIDENCE RESPONSE POLICY AND PROCESSES.

Timeline of events required as part of STC GDPR Policy

Monthly:

All email enquiries folders to be emptied and data requiring retention to be transferred to the relevant email folder or database by the Admin Assistant, Deputy Clerk, Clerk and Community Centre staff.

All hard copy enquiry forms to be deleted and shredded. Data requiring retention is to be transferred to the relevant email, digital folder or database and to be stored digitally by the Admin Assistant, Deputy Clerk, Clerk and Community Centre staff.

All information deleted to be recorded by the information processors in the STC Data Log, which is to be stored electronically.

The Data Information Officer to monitor the tasks above have been completed and sign the data log to this effect.

Annual:

Review and update the Internal Register of Processing Activities.

Ensure the relevant privacy notices and consents are in place for the processing activities identified in the Internal Register of Processing activities. Update the GDPR Document Index with new notices etc.

Review and identify risk in a Personal Data Audit Complete an Annual financial Risk assessment with regard to GDPR as a result of the Personal Data Audit. The completion of this task to be recorded in the STC Data log.

To review the signage for the CCTV in all relevant council buildings and ensure it continues to be compliant with GDPR.

To complete a SAR exercise, evaluate and review any process changes needed to ensure the council is able to comply with SAR.

To prepare an annual report for STC in October containing information on the Annual Review:

- The outcomes of the Annual audits
- The outcome of the Financial Risk Assessment with regard to GDPR and the council's data processing activities
- An account of the number of SARs received and completed within the prescribed timescale
- Any changes required to STC GDPR policy or process as a result of the review.
- Forecast if a DIPA is needed as a result of projects identified in the Town plan or business plan for the following year.
- Budget recommendations for GDPR requirements for the following year for the budget Sub-committee.

As and when required:

Record SAR requests in the SAR log including whether compliance took place within the time limits prescribed.

This policy document is written with current information and advice. It will be reviewed at least annually after the annual information audit has taken place or when further advice is issued by the ICO.

All employees, volunteers Councillors and co-opted committee members are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

All employees, Officers, volunteers, Councillors and co-opted committee members will sign to show they have read and understood the GDPR policy and their agreement to abide by the policy.

I agree to abide by Sheringham Town Council GDPR Policy and in fulfilling my role, follow the Council's GDPR processes. In the event of a personal data breach, I agree to inform the Data Information Officer (DIO) at the earliest opportunity on discovering the breach.		
Full Name	Signature	Date
DIO Full Name	Signature	Date