DINNINGTON ST JOHN'S TOWN COUNCIL

INFORMATION & DATA PROTECTION POLICY

Incl. SECURITY INCIDENT RESPONSE POLICY

MARCH 2024

Adopted: 9th February 2021
Reviewed: 11th March 2024

Information & Data Protection Policy

Introduction

In order to conduct its business, services and duties, Dinnington St John's Town Council (DSJTC) processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

DSJTC will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Town Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

DSJTC recognises it must, at times, keep and process sensitive and personal information about both employees and the public; it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulations (GDPR) which become law on 25th May 2018 and will, like the the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Town Council with legitimate reasons for using personal information.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.
That may be an employee, prospective employee, associate or prospective associate of DSJTC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, card transactions and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Town Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
• organising, adapting or altering it
• retrieving, consulting or using the information or data
• disclosing the information or data by transmission, dissemination or otherwise making it available
• aligning, combining, blocking, erasing or destroying the information or data regardless of the technology used.

DSJTC processes **personal data** in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- monitor its activities including the equality and diversity of its activities

- fulfil its duties in operating the business premises including security
- assist regulatory and law enforcement agencies
- process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Town Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?
The Town Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Town Clerk.

- Email: clerk@dinningtonstjohns.org
- Phone: 01909 564169
- Correspondence: The Town Clerk, Dinnington St John's Town Council, 64 Laughton Road, Dinnington, Sheffield, S25 2PS

Diversity Monitoring

DSJTC monitors the diversity of its employees, and Councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It undertakes similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria and will not be made available to others involved in the recruitment

process. Anonymised data derived from diversity monitoring will be used for monitoring purposes and may be published and passed to other bodies.

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with DSJTC, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however where ever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Town Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information

General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e)
Processing is with consent of the data subject, or
Processing is necessary for compliance with a legal obligation.
Processing is necessary for the legitimate interests of the Council.

Information Security

The Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies.

We will only keep data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted.

Children
We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Rights of a Data Subject

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting our Town Clerk or Data Protection Officer:

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: Town Clerk.

Information Deletion: If the individual wishes the Town Council to delete the information about them, they can do so by contacting the Town Clerk.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Town Clerk or Data Protection Officer.

The Town Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Town Clerk, Data Protection Officer or the Information Commissioners Office **casework@ico.org.uk** Tel: 0303 123 1113.

The Council will always give guidance on personnel data to employees through the employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of the council and its committees are subject to statutory notice being given on notice boards and the council's website. The Council publishes an annual programme each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its website or at its offices.

Occasionally, council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council, but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information

The Council will, as necessary, undertake checks on both staff and Members with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency

The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

“Public data” means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council’s decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:

Demand led: new technologies and publication of data should support transparency and accountability
Open: the provision of public data will be integral to the Council’s engagement with residents so that it drives accountability to them.
Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. DSJTC exceeds this turnover but will never the less ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities
- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

Based on a model policy issued by the SLCC

SECURITY INCIDENT RESPONSE POLICY

1. A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

Security Breach Response

2. Whenever a data breach (or potential data breach) is identified the Clerk is to be notified immediately. If the Clerk is unavailable, the Chair or Vice-Chair is to be informed. The person notified of the breach is to take the following actions as soon as possible:

    a. Complete the attached Data Breach Reporting Form and ascertain as much information as possible regarding the breach, for example:

        i. Name of person reporting the breach.
        ii. How the breach was identified and when (date and time).
        iii. Time the breach was reported to the council.
        iv. The nature of the data that has been breached.
        v. When the data was breached.
        vi. How the data was breached and by whom (if appropriate).
        vii. Unintended recipients of the data (if known).
        viii. The potential damage to the individual whose data has been breached and the council (if known).
        ix. Any actions taken to close the breach and repair any damage to any individual.
        x. Any other relevant information.

    b. **DO NOT DESTROY ANY POTENTIAL EVIDENCE.**
    c. Check the physical security of any premises if appropriate.
    d. Report full details of the breach to the Information Commissioner's Office (ICO) if required **within 72 hours** of the breach being reported to the council at www.ico.org.uk or by calling 0303 123 1113. Guidance on the types of breaches to be reported to the ICO can be found on their website. Even if the breach is not required to be reported to the ICO the council should nevertheless follow this action plan to identify and learn any lessons that could prevent a more serious breach of personal data in the future.
    e. Take any actions as advised by the ICO.
    f. Keep a full detailed log of the dates and times of all actions taken.
    g. Inform all other council members (and Clerk if not already aware) of the data breach and any actions taken/to be taken and by whom.
    h. If appropriate, report to the police.
    i. Inform the council's insurers and ensure they are content with the plan of action.
    j. Identify and take any other immediate actions required to close the data breach and maintain security of other personal data held by the council.
    k. Ensure the subject(s) of the data breach are informed as soon as is appropriate (seek advice of ICO, insurers, police etc.) of both the breach and the information that has been leaked.
    l. If felt necessary, convene an emergency council meeting to discuss and record the breach and, if required, appoint two councillors not involved in the breach to investigate the full facts surrounding the breach and potential liabilities to third parties (if no obvious candidates are available, consideration to appointing councillors from

another authority should be considered). The council should also consider whether it is necessary to seek any specialist legal and/or technical (e.g. forensic IT) advice.

m. The investigators should produce a full report outlining the facts of how the data was breached along with recommendations to ensure there is no repeat breach and, also, whether the council should consider any action against either the Clerk or any members.
n. Seek the advice of RMBC re the best way to handle and control any potential press interest.

DINNINGTON ST JOHN'S TOWN COUNCIL

Data Security Breach Reporting Form

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

Example: Reportable theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	

Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	

Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	