WESTON-SUPER-MARE TOWN COUNCIL

# GDPR AND DATA BREACH POLICY

## Statutory

**History of Policy Changes**

| Date | Version | Author | Origin of Change e.g. change in legislation | Changed by |
|---|---|---|---|---|
| June 2023 | V1 | Town Clerk | | M. Nicholson |
| June 2025 | V2 | Town Clerk/CEO | | H. Morton |

This policy applies to Weston-super-Mare Town Council

| | |
|---|---|
| Date policy adopted | June 2025 (F&GP) |
| Review cycle | Annually |
| Review date | June 2026 |

**Contents**

## 1. Aims

Weston-super-Mare Town Council are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

Weston-super-Mare Town Council are registered as a data controller with the Information Commissioner. The details of the Town Council's Data Protection Officer can be found at paragraph 6.

## 2. Scope

This policy applies to anyone who has access to data and/or is a user of the Town Council ICT systems, both in and out of the organisation, including staff, councillors', other community users.

This policy is also intended to serve as the appropriate policy document for the processing of Special Category Data and Criminal Record Data (where applicable).

This policy applies to all personal data for which the Town Council is the Data Controller, regardless of whether it is in paper or electronic format.

## 3. Definitions

**Personal data** - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The Town Council may process a wide range of personal data of staff (including councillors' and volunteers) as part of its operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our Privacy Notice.

**Special category personal data** - Formerly known as "sensitive personal data", Special Category Data is information that might not necessarily identify a person, but is a lot more sensitive to that person. These are:

- racial or ethnic origin
- political opinions
- religious / philosophical beliefs
- trade union membership
- genetic data
- biometric data (for identification purposes)
- health data (mental and physical)
- sex life or sexual orientation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which can be found on our website. Examples of the types of special category data we hold may be found at Appendix 1.

**Data Subject(s) -** The Data Subject is the person about whom the personal data relates or identifies.

**Data Processing -** Data Processing is an over-arching term that means "doing something" with personal data. This commonly includes:

- Collecting or collating the data
- Analysing the data
- Sharing the data
- Storing the data
- Destroying the data
-
-
- **Controller -** The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

**Data Processor -** is occasionally a person, but more commonly an organisation commissioned by a Data Controller to carry out their data processing on behalf of the Data Controller. These are usually software providers such as Microsoft, or contracted out services such as an insurance company. Essentially, a Data Processor is acting as an extension of the Data Controller, so must operate under the Data Controller's instructions, and under the terms of a Data Processing Agreement.

**Data Sharing -** means *giving* it to another Data Controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the Data Controller for that information, and therefore makes the decisions over what they will do with it.

Note, we do NOT *share* data with our Data Processors, as these are processing it under our Data Controllership.

**Data Breach -** The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, we consider any failing of one of the Data Protection Principles (Article 5 of GDPR) as a GDPR breach, so could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of GDPR).

**Data Processing Agreement –** a legally binding contract between the Data Controller and its Data Processor. This contract defines exactly how the Data Controller expects the Data Processor to process its personal data, and follow standard contract clauses.

**Data Sharing Agreement -** a non-legally binding written agreement between Data Controllers where there is regular sharing of personal data. The Sharing Agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, the how the data will be shared.

## 4.Roles and Responsibilities

Data Protection is the responsibility of all staff within the Town Council. The **Councillors** have overall responsibility for ensuring that our staff comply with all relevant data protection obligations.

**All other staff (as defined in scope)** - All staff are responsible for:

- Familiarising themselves with and complying with this and related policies. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by the Town Council for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; and locking devices when they are temporarily left unattended at any point (Windows Button □ + L is a handy shortcut);
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Deleting any data they hold in line with this policy, and the retention schedule;
- Informing the Town Council of any changes to their personal data, such as a change of address;
- Reporting to the CEO or in their absence the Data Protection Officer in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment, please see - *Sharing Personal Data* (section 10).

### Data Protection Officer

- The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, The Data Protection Officer is Paul Russell and he is responsible for the following tasks;

- Informing and advising the Town Council, any processor engaged by the Town Council as data controller, and any employee of the TownCouncil who carries out processing of personal data, of that person's obligations under the legislation;

- Providing advice and monitoring for the carrying out of a data protection impact assessments;

- Co-operating with the Information Commissioner's Office, acting as the contact point for the Information Commissioner's Office monitoring compliance with policies of the Town Council in relation to the protection of personal data monitoring compliance by the Town Council with the legislation.

- In relation to the policies mentioned above, the data protection officer's tasks include:-
    (a) assigning responsibilities under those policies,
    (b) raising awareness of those policies,
    (c) training staff involved in processing operations, and
    (d) conducting audits required under those policies.

- The Town Council must provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

## 4. Data Subject Rights

In all aspects of its work, the Town Council will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Town Council's work. Subject to exceptions, the rights of the data subject as defined in law are:

1. *The Right to be informed.*

   The Town Council advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

2. *The Right of access*

   An individual when making a subject access request (SAR) is entitled to the following;

   - Confirmation that their data is being processed;
   - Access to their personal data;
   - Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

   The Town Council must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

3. *The Right to rectification*Individuals have the right to ask us to rectify information that they think is inaccurate or incomplete.

   The Town Council has a duty to investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further 2 calendar months can be justified.

4. *The Right to erasure*

   Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

   - The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
   - The information is no longer required by the Town Council;
   - The Town Council has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the Town Council to continue to process it.

   The Town Council will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or a number of requests have been received from the individual.

5. *The Right to restrict processing*

   This is not an absolute right. An individual may ask the Town Council to temporarily limit the use of their data (for example, storing it but not using it) when it is considering:

   - A challenge made to the accuracy of their data, or
   - An objection to the use of their data.

   An individual may also ask the Town Council to restrict the destruction of a record, if they wish it to be retained beyond the normal retention period.

   In addition, the Town Council may be asked to limit the use of data rather than delete it:

   - If the individual does not want the Town Council to delete the data but does not wish it to continue to use it;
   - In the event that the data was processed without a lawful basis;
   - To create, exercise or defend legal claims.

6. *The Right to data portability*

   An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The Town Council only has to provide the information where it is electronically feasible.

7. *The Right to object*

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out for the exercise of official authority
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. The Town Council will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress

## 5. Data Protection Principles

Data protection legislation is based on seven key data protection principles that Town

Council complies with. The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – The Town Council will explain to individuals why the Town Council needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The Town Council reviews its documentation and the basis for processing data on a regular basis
- **Collected for specified, explicit and legitimate purposes** – The Town Council explains these reasons to the individuals concerned when it first collects their data. If the Town Council wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. The Trust will document the basis for processing.
- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed –** The Town Council must only process the minimum amount of personal data that is necessary in order to undertake its work.
- **Accurate and, where necessary, kept up to date** – The Town Council will check the details of individuals on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When the Town Council no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
    - We have a retention and disposal/records management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
    - Once the data is no longer needed, we delete it, securely destroy it in line with

our retention and disposal policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – The Town Council implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the IT Acceptable Use & Mobile Device Policy and how data is securely transferred in and out of the Trust's system.
    - We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from any of our premises.
    - Any decision to remove the information must be based on the business need of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category personal data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.
    - If there is no reasonable alternative to removing hard copies from the organisation name's site, the following procedure will apply:
        i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data questionnaires;
        ii. Information will be transported and stored in a lockable case;
        iii. Wherever possible, information that is removed from site will be pseudonymised by using a "key" held by the office on site;
        iv. We adopt a risk- based approach, for example hard copy personal data with lower sensitivity may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. Health data) must be kept on the staff member's person at all times.
        v. Special category data must be returned to the Town Council premises at the end of the working day. If this is not practicable, and a staff

            member needs to retain the information in their personal possession, this must be discussed in advance with a member of SMT including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SMT must record their decision.
        vi. Data will be tidied away when not in use and not left out.
        vii. Only those who have need to access the data concerned will be granted permission and access to it.

    - **Accountability –** The Town Council complies with its obligations under data protection laws including the GDPR and regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance Processing Personal Data

In order to ensure that the Town Council's processing of personal data is lawful, it will always identify one of the following six grounds for processing **before** starting the

processing:

- The individual has freely given clear consent. The Town Council will seek consent (where appropriate) to process data.
- The data needs to be processed so that the Town Council can fulfil a **contract** with the individual, or the individual has asked the Town Council to take specific steps before entering into a contract;
- The data needs to be processed so that the Town Council can comply with a **legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual, i.e. to protect someone's life;
- The data needs to be processed so that the Town Council, as a public authority, can **perform a task in the public interest, or carry out its official functions**;
- The data needs to be processed for the **legitimate interests** of the Town Council or a third party where necessary, balancing the rights of freedoms of the individual. However, where the Town Council can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

### 5.1 Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the GDPR. The grounds that we may rely on include:

a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.
c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;
d) Processing relates to personal data which are **manifestly made public** by the individual;

Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

e) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision- making process.

f) These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):
   - Statutory and government purposes
   - Safeguarding of children or individuals at risk
   - Legal claims
   - Equality of opportunity or treatment
   - Counselling
   - Occupational pensions

g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

**h)** Processing is necessary for reasons of **public interest in the area of public health;**

i) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

### 5.2 Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or
- Consent – where freely given. The Town Council acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

## 6. Third Parties with Access to Personal Data

Please refer to the Town Council Privacy Notice(s) for details of who, aside from the Town

Council, has access to the personal data processed.

- **Data Sharing**

  The Town Council will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

  - The Town Council will share data if there is an issue with a staff member or third party, for example the safety of staff or others at risk;
  - The Town Council will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so.

The Town Council may also disclose personal data to law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided or it is otherwise fair and lawful to do so.

The Town Council may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects councilors, volunteers or staff.

- **Third-Party Processors**

The Town Council suppliers and contractors including its Data Protection Officer may need data to provide services. When third parties are processing personal data on behalf of the Town Council, the Town Council will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares where there is regular sharing;
- Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Town Council.

.

## 7. Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred, or a "near-miss" has

occurred, the staff member must inform the CEO, in the first instance, or a member of SMT and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

This policy applies to all employees of the Town Council including contract, agency and temporary staff, volunteers and employees of partner organisations working for the Town Council. For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

The quick response to a suspected or actual data breach is key. All consumers in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours then this should be reported as soon as practically possible. This should be done through the completion of the reporting form in Appendix 8, which is sent to the CEO, in the first instance, or a member of SMT, who will liaise with its DPO. A separate form, “The Town Council Data Breach Reporting Form” is available to aid communication.

a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches
b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.
c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.
d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.
e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. The organisation's Communications / Press Team may also be notified to handle any queries and release statements.

A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Whether controls are sufficient
- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary

If necessary a report recommending any changes to systems, policies and procedures will be considered by the senior management board. This will include the decision on whether to report to the regulator and affected data subjects.

Phases (b) to (e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported.

## 8. Destruction of records

The Town Council adheres to its retention policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

The Town Council will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

Where the Town Conucil deletes electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

## 9. Training

To meet its obligations under Data Protection legislation, the Town Council will ensure that all staff, volunteers, Councillors receive an appropriate level of data protection training as part of their induction. Permanent members of staff will receive Data Protection training at least every 12 months. Those who have a need for additional training will be provided with it, for example relating to use of systems or CCTV.

Data protection also forms part of continuing professional development. Staff members undertakes regular informal discussions on Data Protection, to ensure key updates are provided where changes to legislation, guidance or the Town Council's processes make it necessary. This will include lessons learned from Data Breaches and Near Misses, preventative measures to avoid them, and other best practice as advised.

Regular information emails will be sent to all staff to raise awareness of GDPR and Cyber-security issues and remind them of key processes.

## 10. Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Town Council's overall compliance with data protection law, the Town Council is responsible for the day to day implementation of the policy and for making the Data Protection Officer aware of relevant issues which may affect the Town Council's ability to comply with this policy and the legislation.

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

## 11. Complaints

The Trust is always seeking to implement best practice and strives for the highest standards. The Trust operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Trust's complaints policy may be found on its website.

There is a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the Trust or via the Trust's DPO.

The ICO is contactable at:

Wycliffe
House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

## 12. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office

## 13. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Retention & Disposal / Records Management Policy
- Mobile device Policy
- Privacy Notices
- Safeguarding Policy
- IT Acceptable Use Policies
- Social Media Policy
- Password Policy

- Consent / Permissions Form
- Admissions Form

## 14. Review

This policy is reviewed annually by the Town Council and where materially amended is consulted on, where necessary and upon; Change of Data Protection Officer, Change of Legislation. We will monitor the application and outcomes of this policy to ensure it is working effectively. Review this Policy

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the CEO/Town Clerk.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with the CEO/ Town Clerk, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

## Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include in

Staff health data and information
Staff applications forms
HR files including disciplinary and capability proceedings which may include DBS and right to work checks, health and equal opportunities data (disability, race, ethnicity, sexual orientation)
Accident reporting documentations

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as do our Privacy Notices which may be found on the Town Council website.

## Appendix 2 - Subject Access Request Procedures

The organisation shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from the DPO.

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain proof of identity (once this step has been completed the clock can start)
3. Engage with the requester if the request is too broad or needs clarifying
4. Make a judgement on whether the request is complex and therefore can be extended to a 2 month response time
5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), 2 months if complex; and

b. details of any costs – Free for standard requests, or you can charge if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the Town Council.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer.

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested

**Appendix 3:**

**Appendix 4: Privacy Notice for Staff**

Under data protection law, individuals have a right to be informed about how the Town Council uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at the Town Council.

We, Weston-super-Mare Town Council, are the 'data controller' for the purposes

of data protection law. Our data protection officer is Paul Russell. Email:

paul@microshadevsm.co.uk

***The categories of the Town Council workforce information that we collect, process, hold and share include:***

We process data relating to those we employ, or otherwise engage, to work at the Town Council. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Contract information, start dates, hours worked, post and role

- Bank account details, payroll records, National Insurance number, tax status information and employee/teacher number
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data and reasons for absence
- Copy of driving license
- Photographs
- Data about your use of the Town Council information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

***Why we collect and use this information***

The purpose of processing this data is to help us run the Town Council, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Enable the development of a comprehensive picture of the workforce and how it is deployed

***The lawful basis on which we process this information***

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation

- Carry out a task in the public interestLess commonly, we may also use personal information about you where:
    - You have given us consent to use it in a certain way
    - We need to protect your vital interests (or someone else's interests)

**Special Categories of Personal Data**

Some of the data we collect requires additional legal basis to process, and is known as Special Categories of Personal Data (SCoPD). The categories that we collect are:

- Racial or ethnic origin
- Trade union membership
- Data concerning health

There are additional legal bases for processing these special categories of personal data and these are laid out in our Data Protection Policy.

***Collecting this information***

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain staff workforce information to us or if you have a choice in this.

***Storing this information***

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.
Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Retention Policy

**Why we share staff workforce information**

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

**Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer Paul Russell.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**Further information**

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, Paul Russell email: paul@microshadevsm.co.uk

**Appendix 6: Privacy Notice for Job Applicants**

Under data protection law, individuals have a right to be informed about how the Town Council uses any personal data we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals applying for jobs at the Town Council.

We, Weston-super-Mare Town Council are the 'data controller' for the purposes of data protection law.

Our data protection officer is officer is Paul Russell (see 'Contact us' below).

Successful candidates should refer to our privacy notice for the Town Council for information about how their personal data is collected, stored and used.

**The personal data we hold**

We process data relating to those applying to work at the Town Council. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

**Why we use this data**

The purpose of processing this data is to aid the recruitment process by:

- Enabling us to establish relevant experience and qualifications
- Facilitating safe recruitment, as part of our safeguarding obligations towards staff
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for candidates that require them

**Our lawful basis for using this data**

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the Trust's use of your data.

**Collecting this information**
**While the majority of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.**

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

**How we store this data**

If your application for employment is unsuccessful, the Trust or academy for which you have applied will hold your data on file for 6 (six) months after the end of the relevant recruitment process. At the end of this period your data is deleted or destroyed securely.

If your application is successful, personal data gathered during the recruitment process will be transferred to your human resources file (electronic or paper based) and retained during your employment. The periods and purpose for which your data will be held will be provided to you in a new privacy notice.

**Data sharing**

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as shortlists of candidates for a Head teacher position
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as data protection officer
- Professional advisers and consultants - to help us select the most suitable candidate
- Employment and recruitment agencies - to help us select the most suitable candidate

**Transferring data internationally**

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

**Your rights**

**How to access the personal information we hold about you**

Individuals have a right to make a 'subject access request' to gain access to personal information that the Town Council holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you

- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

**Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data

protection regulations To exercise any of these rights, please contact our data

protection officer.

**Freedom of Information Requests procedures**

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities; and. members of the public are entitled to request information from public authorities.

Under the FOI Act 2000 there are exemptions to protect information that should not be disclosed, for example because disclosing it would be harmful to another person or it would be against the public interest. Some exemptions relate to a particular type of information, for instance, information relating to government policy. Other exemptions are based on the harm that would arise or would be likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests. The exemptions are:

Section 21 – information already reasonably accessible
Section 22 – information intended for future publication
Section 22A – research information
Sections 23 and 24 – security bodies and national security
Sections 26 to 29
Sections 30 and 31 – investigations and prejudice to law enforcement
Section 32 – court records
Section 33 – prejudice to audit functions

Section 34 – parliamentary privilege
Sections 35 and 36 – government policy and prejudice to the effective conduct of public affairs
Section 37 – communications with the royal family and the granting of honours
Section 38 – endangering health and safety
Section 39 – environmental information
Section 40(1) – personal information of the requester
Section 40(2) – Personal information
Section 41 – confidentiality
Section 42 – legal professional privilege
Section 43 – trade secrets and prejudice to commercial interests
Section 44 – prohibitions on disclosure

More detail for each section can be found under the ICO website https://ico.org.uk/for-organisations/foi/guide-to-managing-an-foi-request/exemptions/list-of-exemptions/

There is also an exemption for personal data if releasing it would be contrary to the UK General Data Protection Regulation (the UK GDPR) or the Data Protection Act 2018 (the DPA2018).

The Town Council's main obligation under the Act is to respond to requests promptly, with a time limit acting as the longest time you can take. Under the Act, the Town Council take up to 20 working days to respond, counting the first working day after the request is received as the first day.

There are two separate duties when responding to these requests:

- to tell the applicant whether you hold any information falling within the scope of their request; and
- to provide that information

The Town Council is not always obliged to provide the information. In some cases, there will be a good reason why the Town Council should not make public some or all of the information requested.

The Town Council can refuse an entire request under the following circumstances:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

.

If the Town Council refuses all or any part of a request, a written refusal notice must be sent to the requester. The refusal notice must state whether the Town Council holds information at all, or confirming that information is held but refusing to release it.

More detailed information on how to manage a freedom of information request can be found at:

https://ico.org.uk/for-organisations/foi/guide-to-managing-an-foi-request/

**Subject Access requests**

A Subject Access Request (SAR) policy outlines how an organization handles requests from individuals to access their personal data, as mandated by the General Data Protection Regulation (GDPR) and other relevant data protection laws. The policy should clearly define procedures for recognizing SARs, verifying identities, handling requests, responding within specified timeframes, and addressing potential exemptions.

## Staff requests

### How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the Town Council holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a Subject Access Request request, please contact the Democratic Services Manager on sam.bishop@wsm-tc.gov.uk

### Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

### Procedure

**Logging a Subject Access Request**

Once a subject access request has been received the CEO/Town Clerk or person responsible for responding to the request will log the request on the Subject Access Request Register.The register will be used to track the progress of the subject access request.

**Valid Subject Access Request**

A valid subject access request can be received in any format including but not limited to, in writing, verbally or on social media. An individual does not need to use any specific wording to define their request, however the Town Council will offer a Subject Access Request form to assist in ensuring the Town Council will have all relevant information to process the request. A Subject Access Request can only be fulfilled when the Town Council have validated the identity of the individual making the request and have all of the information required to provide the information requested.

Where the Subject Access Request is not valid as documented in the section above the CEO/Town Clerk or person responsible for responding to the request will contact the person making the request, to seek further information.

Once the CEO/Town Clerk or person responsible for responding to the request has received all the information they need and sufficient information to verify the data subject's identity, the Town Council has one month to provide the information requested.

Correctly identifying the data subject. Before disclosing any personal information, the CEO/TownClerk or person responsible for responding to the request must verify the identity of the data subject.

Whilst it is important that the Town Council does not send copies of personal information to people who are not the data subject, the Town Council must not appear obstructive. **The Data Protection Act** requires the Town Council to take "reasonable measures" to verify the identity of a data subject. The CEO/Town Clerk or person responsible for responding to the request shall keep a record of what measures they taken to verify the identity of the person making the request.

**Locating personal information for the Subject Access Request**

The CEO/Town Clerk or person responsible for responding to the request will work to identify systems where personal data of the data subject is being held, as well as identifying the means by which the personal data can be extracted.

When the systems have been identified, CEO/Town Clerk or person responsible for responding to the request will carry out searches to identify personal data held on the data subject and export to a common area so that personal data can be combined before the data can be screened prior to disclosure to the data subject.

**Reviewing Personal Information and what cannot be disclosed as a result of a Subject Access Request**

Once information has been collated on what the Town Council hold about a data subject this information will be examined by the Data Protection Officer to establish if it should be

disclosed. This must be done on a case-by-case basis for each individual piece of information. In some cases, we might disclose only parts of particular documents. This shall include checking that the record is actually about the person concerned and not about someone else with the same name, screening out any duplicate records.

Where there are instances where personal information does not require to be disclosed. The CEO/Town Clerk or person responsible for responding to the request will determine if any of the exemptions apply before releasing personal information.

Where a document contains personal data about a number of individuals, including the data subject, they we will not disclose the information about the third parties to the data subject. If the record is primarily about the data subject, with incidental information about others, then third-party information will be redacted. If the record is primarily about third parties, then the document will be withheld if redacting is not possible.

Where possible third parties will be contacted to obtain consent to disclose the document if possible.

**Sending Personal Data to Data Subject**

Once the Data Protection Officer has identified all of the information that can be sent in response to a SAR, one final review will be undertaken of this information as a collection of data.The personal data of the data subject will be sent to the data subject as provided on the Data Subject Access Request form.

**Complaints**

The Town Council take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer, Paul Russell

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

- Paul Russell email: paul@microshadevsm.co.uk Appendix 10: Seven Golden Rules to Information Sharing

The following ‘golden rules’ have been taken directly from the following government guidance;

“Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and cares” HM Government, July 2018

The seven golden rules for sharing information

- Remember that the General Data Protection Regulations (GDPR),Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
- Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
- Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Under the GDPR and Data Protection Act 1998, you may still share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
- Consider safety and wellbeing: Base your information sharing decisions on considerations of the safety and wellbeing of the individual and others who may be affected by their actions.
- Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
- Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.