Watton Town Council

Policy and procedure for personal date breaches

June 2024

---

1. POLICY OVERVIEW

1.1 This policy will apply to all the personal data that is collected and used by Watton Town Council from time to time (referred to as "**WTC**", "**we**", "**us**", "**our**").

1.2 As an organisation, we value the personal information that is entrusted to us by members of the public, our staff, our councillors and officers, our contacts and other third parties. It is extremely important that we uphold that trust in the way in which we handle, use, store and protect personal data.

1.3 Given the public services which we provide, and the ongoing contact we have with members of the public, we recognise that we are likely to collect and process personal data on a wide range of individuals on a day-to-day basis. In light of this position, it is fundamental that we take data protection seriously.

1.4 To this end, we are committed to adopting high standards in our protection of data and in addressing privacy concerns. Not only are we putting in place appropriate technical and security measures, but also ensuring that we have privacy and the protection of data at the heart of our decision-making processes across the organisation.

1.5 We are dedicated to being open and transparent with individuals about how we use and handle their information.

1.6 It is also important to recognise the importance of our staff when considering data protection compliance. We will ensure that we provide training to staff who handle personal information as part of their role. Equally, we will treat it as a disciplinary matter if they misuse or fail to take proper care of personal information.

2. GENERAL DATA PROTECTION REGULATION ("GDPR")

2.1 The GDPR came into effect on **25 May 2018**, and is implemented in the United Kingdom by the Data Protection Act 2018.

2.2 This policy, and other data protection policies operated by us, have where possible been written with the implementation of the GDPR in mind, and in particular its

implementation within the domestic jurisdiction of the United Kingdom following the UK's exit from the European Union.

2.3 However, please note the GDPR is now under the direct jurisdiction of the UK, and is now implemented as the retained EU law version of the GDPR within the United Kingdom ("**UK GDPR**"). There may be changes from time to time to either the GDPR and/or the UK GDPR, and it may be that changes are not mirrored or replicated in both versions. This policy, and WTC's other data protection policies, will need to be reviewed and updated an ongoing basis to ensure compliance, and all Personnel (as defined below) should seek assistance from the Data Compliance Manager if unsure about which legislation applies, or if unsure about any part of this policy, or any other data protection policy, operated by WTC.

2.4 Fundamental to the UK GDPR is a high standard of accountability. All organisations, including WTC, will be required to demonstrate and evidence how they comply with the data protection principles (as set out further in this policy). Compliance with this policy (and our other data protection-related policies) will assist WTC in doing so.

2.5 Please note that all references to the GDPR and the UK GDPR in this policy also includes references to the Data Protection Act 2018.

3. ABOUT THIS POLICY

3.1 This policy applies to all staff unless otherwise indicated. This policy therefore applies to WTC's officers, councillors, managers, employees (whether part-time or fixed term), consultants, contractors, agents, casual and agency staff (collectively referred to as "**Personnel**", "**you**", "**your**").

3.2 This policy may be amended from time to time and Personnel will be directed to certain parts of the policy as and when it is reviewed and updated.

3.3 This policy does not form part of any employee's contract of employment or any other Personnel's contractual terms.

3.4 The Data Compliance Manager of WTC will have overall responsibility for data protection compliance within the organisation and for ensuring this policy (together with other data protection-related policies operated by WTC) are

adhered to and comply with the relevant legal obligations. The Data Compliance Manager's details are set out below:

Name	Position	Contact Details
Jane Scarrott	Town Clerk & Data Compliance Manager	01953 881007 clerk@wattontowncouncil.gov.uk Watton Town Council, Wayland Hall, Middle Street, Watton, Norfolk IP25 6AG

Please contact the Data Compliance Manager with any questions about the operation of this policy, a data breach or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

3.5 This policy will be reviewed from time to time by the Data Compliance Manager, and the officers and councillors of WTC, to ensure that its provisions continue to meet the relevant legal obligations and reflect best practice.

3.6 All managers and supervisors have a specific responsibility to operate in accordance with the provisions set out in this policy and to ensure that all Personnel under their supervision understand the standards of behaviour expected of them, and to take action when behaviour falls below those requirements.

3.7 We recognise that the correct and lawful treatment of personal data will maintain confidence in the Council as a local authority and will assist us in providing quality local public services ,whilst upholding the security of personal data. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. **It is important to note that even though WTC is a local authority, it can still be exposed to serious and highly detrimental fines and penalties, the value of which will depend on the nature of the breach, for failure to comply with the provisions of the UK GDPR.**

4. KEY DATES

4.1 This policy was last reviewed by the officers and councillors of WTC, and the Data Compliance Manager, on [●] 2024.

4.2 This policy is next due to be reviewed on [●].

5. RECOGNISING A DATA BREACH

5.1 A data breach can happen for any number of reasons, and it is important that all Personnel are able to recognise a data breach and know to whom they should report any suspected or actual data breaches.

5.2 Under the UK GDPR, the legal definition of a personal data breach is widely defined:

"*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*".

This therefore includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

5.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

5.4 A data breach, amongst other things, can include the following:

5.4.1 Loss or accidental destruction of files or equipment on which data is stored;

5.4.2 Theft of files or equipment on which data is stored;

5.4.3 Inappropriate access controls allowing unauthorised use;

5.4.4 Equipment failure;

5.4.5 Unforeseen circumstances such as a fire or flood;

5.4.6 Hacking attack;

5.4.7 Erroneously sending an e-mail to the wrong recipient;

5.4.8 Unauthorised collection or use of personal data; and/or

5.4.9 "Blagging" offences where information is obtained by deceiving the organisation who holds it.

5.5 Under the UK GDPR and other applicable data protection legislation, any of the above may still be a data breach even if WTC can establish that no one has accessed, or can access, the personal data. On that basis, a cautious approach must always be adopted by Personnel in relation to personal data breaches. If you have any doubt, it should be reported as set out in this policy.

6. WHEN TO REPORT A BREACH

6.1 When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then we must notify the ICO. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we must document it. **As such, all Personnel must follow the processes and procedures in this policy so that we have all relevant information.**

6.2 Failure to notify

6.2.1 We recognise that the correct and lawful treatment of personal data will maintain confidence in our organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

6.2.2 **It is important to note that failing to notify a breach when required to do so can result in a significant fines and penalties for WTC.**

6.2.3 For this reason, detecting and reporting a breach, on time and in accordance with this policy; and providing the necessary details is vital.

6.3 Dedicated person

Our dedicated person for managing breaches is currently the Town Clerk, Jane Scarrott. Jane can be contacted on 01953 881007 and clerk@wattontowncouncil.gov.uk. We will notify you if the dedicated person changes.

6.4 Relevant supervisory authority

The relevant supervisory authority for our processing activities is the ICO.

6.5 Who reports a breach

The officers of WTC, along with the councillors for the time being and the Data Compliance Manager, will determine whether or not a breach notification needs to be made in accordance with the table at paragraph 7.2.5 below, and if so, the content of that notification. In doing so, the officers, councillors and the Data Compliance Manager may liaise with WTC's legal advisers. **Please note that Personnel (including individual councillors) should NOT notify the ICO (or any other Supervisory Authority), or any affected individuals without the prior consent of the officers and Data Compliance Manager of WTC.**

7. PROCEDURE

7.1 It is essential that all Personnel follow the reporting structure set out below in the event of any actual or suspected breach.

7.2 In general terms, on identifying a breach:

7.2.1 Determine who needs to be notified;

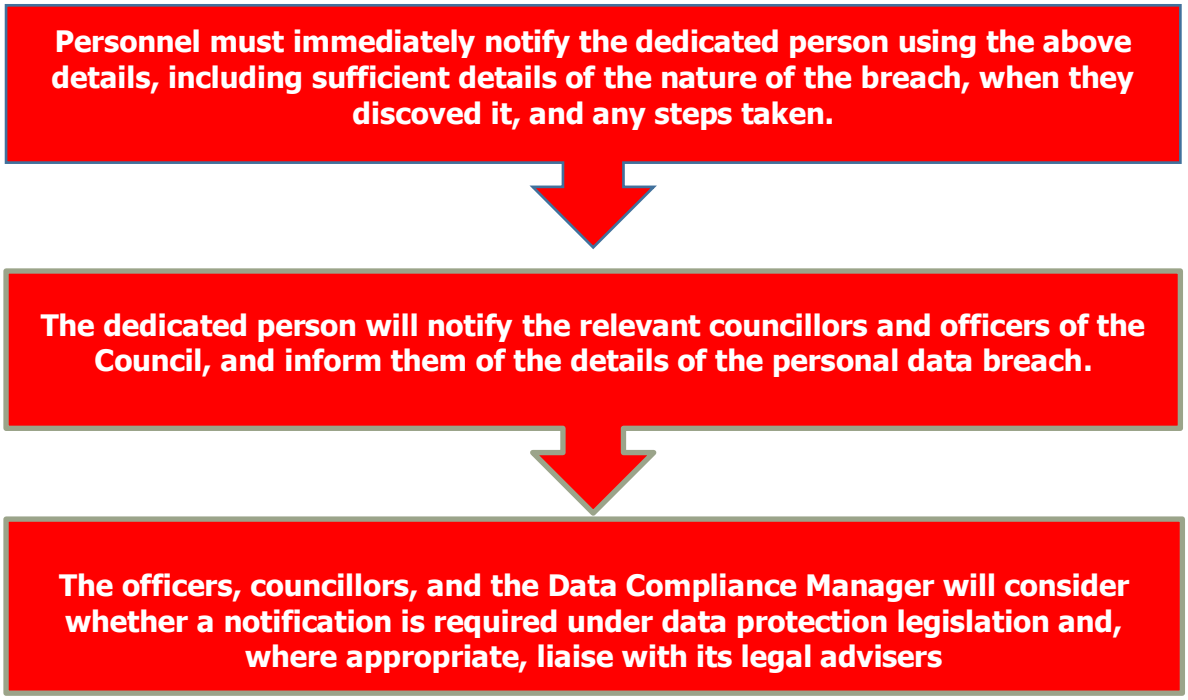
7.2.2 **Always** notify our dedicated person (whose details are above);

7.2.3 the ICO may be notified in accordance with paragraph 6.5 (and in any event, only by the officers and councillors of WTC (acting together) and/or the Data Compliance Manager);

7.2.4 **Sometimes** individuals may also be notified: when there is a high risk of their rights and freedoms being adversely affected, they must be informed without undue delay – this notification will be made in accordance with paragraph 6.5 (and in any event, only by the officers and councillors of WTC (acting together) and/or the Data Compliance Manager);

7.2.5 A record must be kept of any personal data breaches, regardless of whether we are required to report it.

7.3 Our reporting structure is as follows:



8. CONTAINMENT AND RECOVERY

8.1 Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with our customers or other third parties.

8.2 Our IT providers will assess and establish whether there is anything that can be done to recover any losses and limit the damage the breach may have caused. This could involve the use of back up tapes to restore lost or damaged data or ensuring that personnel recognise when someone tries to use stolen data to access accounts.

9. RECORDING DATA BREACHES

9.1 We will maintain a collective internal breach register in order to comply with our obligations under the UK GDPR. This register will document each breach incident including when the breach occurred, the facts relating to the personal data breach,

its potential implications, whether anyone was notified (and if not, why not) and the remedial action taken.

9.2 Our dedicated person will take ownership of a breach once they have been notified and will be responsible for entering the details into our data breach register.

9.3 The ICO may at any time request to review this register to assess how we comply with our data breach notification obligations, so it is crucial to ensure that it is properly maintained.

9.4 Our data breach register is held at the Town Council's offices at Wayland Hall, Middle Street, Watton, Norfolk IP25 6AG.

10. REPORTING DATA BREACHES

10.1 WTC recognises that informing people and organisations about a data breach can be an important element in any breach management strategy, and can help to ensure that we are acting transparently with regards to the way that we handle personal data.

10.2 A decision about who to notify of breaches should be taken in line with the following requirements under the UK GDPR:

Who to notify?	When?	Exemption?
Supervisory Authority (in the UK, the ICO) *(if we are the controller)*	**Where required, without undue delay and, where feasible, not later than 72 hours after becoming aware of it.**	No notification is required if the breach is unlikely to result in a **risk to the rights and freedoms** of natural persons.
Affected Data Subjects *(if we are the controller)*	Where required, without undue delay (however allowing for time where WTC may be implementing appropriate measures against continuing breaches).	No notification is required if: (a) the breach is **unlikely to result in a high risk for the rights and freedoms** of data subjects; (b) appropriate technical and organisational protections were in place at the time of the incident (e.g. encrypted data); or (c) reporting would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed).

Other Controllers *(if we are the processor)*	Without undue delay	None.

10.3 As set out in paragraph 6.5, the dedicated person and the officers and councillors of WTC (acting together) will be responsible for any notification. **Please do not make any notification to the ICO, the affected individuals or anyone else without the prior written consent of the officers and Data Compliance Manager of WTC.**

10.4 When notifying the ICO (or other supervisory authority) it should be noted that in order to fulfil the reporting requirements, the relevant notification should include:

10.4.1 a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;

10.4.2 details of information communicated to affected individuals (if any);

10.4.3 details of the Data Compliance Manager, and other contact points (as determined by the officers and Data Compliance Manager of WTC) where information may be obtained;

10.4.4 the likely consequences of the personal data breach; and

10.4.5 the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, to mitigate any possible adverse effects.

10.5 The officers and councillors of WTC, along with the Data Compliance Manager, will also consider with our legal advisers as to whether it is appropriate to inform the police of any breach.

11. CHANGES TO THIS POLICY

We reserve the right to change this data breach policy at any time so please check back regularly to obtain the latest copy of this policy. Where appropriate, we will notify you of the changes to this policy as soon as possible.