HARWICH TOWN COUNCIL

DATA PROTECTION POLICY

THIS DOCUMENT OUTLINES THE POLICY ADOPTED BY HARWICH TOWN COUNCIL

Date of policy: September 2025
Approving committee: Finance and General Purposes
Date of committee meeting: 23.09.25
Policy version reference: Version 2
Supersedes: Data Protection December 2024
Policy effective from: September 2025
Date for next review: September 2028

Data Protection Policy

Harwich Town Council ('the council') aims to ensure that personal information and data is treated lawfully and correctly.

It is the duty of individual employees and members to ensure that personal information held by them and the council, is dealt with in accordance with Data Protection legislation (General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and The Data Use and Access Act 2025).

This policy applies to all officers, members and those engaged in undertaking business with or on behalf of the council. This policy aims to ensure the council continuously complies with all relevant legislation and good practice, in order to successfully protect the data, it holds and processes.

This policy does not apply to the personal data relating to members of the public or other personal data processed for Council business.

The Council has appointed the Clerk of the Council as the person with responsibility for data protection compliance within the Council. Questions about this policy, or requests for further information should be directed to them.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" refers to information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic, biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings

Collecting & Communicating Personal Data

Personal Information will be:

- Processed fairly, lawfully and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to meet the purpose
- Accurate and up to date
- Kept for no longer than is necessary
- Kept secure to maintain integrity and confidentiality
- Processed in a responsible manner

Keeping People Informed

Harwich Town Council's privacy notice is available for download on the website www.harwichtowncouncil.gov.uk/privacy. This notice is under regular review and Harwich Town Council will place any updates on the website. The current privacy notice was last reviewed in July 2025**.**

Personal data shall only be passed onto third parties if consent is obtained. The council will ensure that an individual is aware of their right to be forgotten and can withdraw their consent at any time, for their data to be processed. The council will inform the subject of the potential impact this decision may have, as it may prevent the council being able to provide the service that has been requested.

Consents

A record of all consents will be maintained by the council where this is relied on this as a lawful basis. The central record will be held electronically and updated as necessary. If consent is withdrawn, all records will be destroyed.

Data Breaches

The Clerk is responsible for managing data breaches.

The council has a set procedure for reporting data breaches to both the Information Commissioner's Office (ICO) and any affected data subjects.

In the event of a data breach having been identified/notified *(i.e. when personal data is lost, destroyed, corrupted or disclosed; if data is accessed or passed on without proper authorisation; if the data is made unavailable, e.g. when it has been encrypted by ransomware, accidentally lost or destroyed),* as a result of either accidental or deliberate cause, in the first instance, this will be reported to the Clerk. The cause, source and extent of the breach will be investigated, and its impact evaluated.

If the breach is likely to result in more than an inconvenience to those using the data to undertake their job or there is a risk of adversely affecting any individuals' rights and freedom, the council will report the data breach to the ICO within 72 hours of becoming aware of the breach.

If the extent of the breach is such that the data subject(s) could be significantly affected *(i.e. financial loss, loss of reputation or risk of discrimination)* the data subject(s) will be informed, in writing, without delay.

The Clerk will be responsible for reporting the breach to the ICO following all guidance provided by them in terms of what information must be given. The Clerk will be responsible for notifying any data subject(s) utilising the template data breach response letter.

All data breaches will be documented, along with details of actions taken (if any) whether or not they are reported to the ICO or data subject(s).

Processing Personal Data

When processing the personal data of any individual, the council will fully observe all conditions regarding the collection and use of information to meet the needs outlined under

the General Data Protection Regulations 2018. The council will collect, process and retain data only to the extent that it is required to fulfil operational needs or legal requirements.

An individual will be informed when their personal data is being processed by the council. Every individual whose information is processed by the council, will, at any time, have the right to access it.

Storing & Managing Personal Data

Right to Correction

The council will periodically review the data it processes to ensure it remains accurate and will amend any inaccurate or incomplete data. Individuals have the right to have their personal data corrected/rectified if it is inaccurate or incomplete. If the information has been disclosed to a third party the council, will inform the individual of who their data has been given to and will tell those third parties to correct personal data at accordingly. This will be undertaken periodically, at the least, annually.

Subject Access Request

Individuals are entitled to access the information that the council holds about them. The council will ensure that personal data is easily accessible at all times so an individual receives a timely response. A subject access request form is available from the council.

The Council will provide you with a copy of your personal data and this will usually be in electronic form unless you agree otherwise.

If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the cost of responding to the request.

The Council has the right to request proof of identification before any request is processed and may charge a fee if additional copies of information is required, which will be based on the administrative cost to the Council.

Other rights

You have a number of other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the council's legitimate grounds for processing data.

- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the council to take any of these steps, you should send the request to the Clerk or Chairman of the Council.

Data security

The council takes the security of HR-related personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Confidentiality

Harwich Town Councillors and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject has otherwise given permission. This also applies when using social media or contact with the press. When handling personal data, this must also remain confidential. If a data breach is identified, the ICO must be informed and an investigation will be conducted.

Individual responsibilities

You are responsible for helping the council keep your personal data up to date. You should let the council know if data provided to the council changes, for example if you move to a new house or change your bank details.

Everyone who works for, or on behalf of, the council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with the council's policies.

You may have access to the personal data of other individuals and of members of the public in the course of your work with the council. Where this is the case, the council relies on you to help meet our data protection obligations to staff and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);

- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the council's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

Reviews

The council will periodically review stored personal data and identify any that is deemed inaccurate or no longer required for the purposes for which it was originally obtained. This will include: manual files, electronic files, PC hard drives – both personal and shared and the BT Cloud Phone database.

Disposal of Personal Data

Erasure

Upon request from a data subject, their personal data will be deleted from all sources unless there is a legal obligation to retain this. If the data is required for either statistical or historical purposes, the personal data will be anonymised or removed.

Complaints and Queries

Queries regarding this policy should be addressed to Harwich Town Council's Clerk: info@harwichtowncouncil.gov.uk

If you are not satisfied with the council's response to a subject access request, you can make a complaint using the council's complaints procedure https://www.harwichtowncouncil.gov.uk/your-council/complaints/

You can speak to your local councillor(s) to see if they can resolve the issue for you. If you are unclear who this is, please contact the council offices on 01255 507211 or visit our website https://www.harwichtowncouncil.gov.uk/your-council/councillors/

If you feel the council have not dealt with your complaint in the correct manner, please contact the **Information Commissioner** at:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

This policy will be reviewed every 3 years or as required in accordance with changes in legislation. A review of the compliance and effectiveness of this policy will also be undertaken.

References/Further Information

https://www.gov.uk/data-protection

https://ico.org.uk/