



**Burnham-on-Sea
& Highbridge**

TOWN COUNCIL

Appropriate Policy Document

Date approved: 21st September 2026

Review Date: September 2027

Appropriate Policy Document

Introduction

Burnham-on-Sea and Highbridge Town Council need to process personal data about its current and former staff, Councilors and the customers of its facilities, to carry out its functions. As part of its operations, it is also necessary for the Council to process special category data. Special category data (defined by Article 9 of the UK General Data Protection Regulation (GDPR)) and sensitive data (defined by section 35 of the Data Protection Act 2018 (DPA)) is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Article 10 UK GDPR applies to the processing of personal data relating to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 provides that criminal offence data includes data which relates to the alleged commission of offences and related proceedings and sentencing. Information about victims and witnesses of crime is also included in the scope of data relating to criminal convictions and offences.

This policy meets the requirement in the DPA 2018 for an appropriate policy document which details the lawful basis and conditions for processing and safeguards Burnham-on-Sea and Highbridge Town Council has put in place when processing special category data and criminal offence data.

Description of Data Processed

Burnham-on-Sea and Highbridge Town Council Privacy Statement has more information about the information processed by the Council, the legal basis for processing and what the information is used for.

Special Category Data

The Town Council processes special category personal data under the following legal basis:

- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Council or the data subject in connection with employment, social security, or social protection. For example where the Council processes staff sickness and absences information.
- Article 9(2)f – Legal claims or judicial acts where processing is necessary.

- Article 9(2)(g) – reasons of substantial public interest. For example, to comply with other obligations imposed on the Council in its capacity as a public authority e.g., the Equality Act.
- Article 9(2)(j) – Archiving purposes in the public interest scientific or historical research or statistics.

Section 10(3) of the DPA 2018 sets out that for processing of special categories of personal data and criminal offence data to be necessary for reasons of substantial public interest under Article 9(2)(g) of the UK GDPR, that processing must meet one of the conditions set out in Part 2 of Schedule 1.

The Council processes special category and criminal offence data in the performance of its statutory and corporate functions when the following conditions set out in the following paragraphs of Part 2 of Schedule 1 to the DPA 2018 are met:

- paragraph 6 Statutory and government purposes
- paragraph 8 Equality of opportunity or treatment
- paragraph 10 Preventing or detecting unlawful acts
- paragraph 11 Protecting the public
- paragraph 12 Regulatory requirements relating to unlawful acts and dishonesty etc.
- paragraph 14 Preventing fraud

Criminal Offence Data

The Town Council processes criminal offence data under Article 10 of the GDPR. Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations. All processing might also be for others dependent on the context. The Council may also process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. The processing of such data respects the rights and interests of the data subjects.

Compliance with the Data Protection Principles

In accordance with the accountability principle, the Council maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. The Council will carry out data protection impact assessments (where appropriate) in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and default. The Council follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for processing, as follows:

Accountability Principle

The Council has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of the Town Clerk as data protection officer
- Taking a 'data protection by design and default' approach.
- Maintaining documentation of processing activities.

- Adopting and implementing data protection policies. Implementing contracts with data processors where appropriate.
- Implementing appropriate security measures in relation to the personal data.
- Carrying out data protection impact assessments (where required).
- Regular review of accountability measures.

Principle (a): Lawfulness, Fairness and Transparency

The Council ensures that all personal data is processed lawfully, fairly, and in a transparent manner. To demonstrate compliance with this principle, the Council maintains clear documentation, defined responsibilities and accessible information for individuals.

Governance and Documentation

The Council maintains appropriate records and policies to support lawful and fair processing, including:

- A comprehensive Article 30 Record of Processing Activities (ROPA) and associated Data Map.
- Adopted Data Protection and Retention policies.
- Regular review of processing activities to ensure they remain accurate, necessary and compliant.
- Designated responsibility for data protection compliance within the organisation.

The Council keeps this Appropriate Policy Document under review and retains it in accordance with statutory requirements.

Transparency

The Council provides clear and accessible information about how personal data is processed, including:

- The lawful basis for each processing activity.
- The purposes for which personal data is used.
- The categories of data involved and who it may be shared with.

This information is made available through the Council's Privacy Statement, and this policy document, ensuring individuals understand how their data is handled.

Principle (b): Purpose Limitation

- The Council processes personal data for purposes of substantial public interest as explained above when the processing is necessary to fulfil statutory and corporate functions. The Council is authorised by law to process personal data for these purposes.
- Where the Council shares data with another organisation, the Council shall document that sharing and implement a data sharing agreement (where required).
- The Council shall not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): Data Minimisation

- The Council shall collect personal data necessary for the relevant purposes and ensure it is not excessive. The information processed is necessary and proportionate.
- Where personal data is provided to the Council or obtained but is not relevant to our stated purposes, it will be erased.

Principle (d): Accuracy

- The Council shall ensure that where personal data is identified as inaccurate or out of date, having regard to the purpose for which it is being processed, the Council will take every reasonable step to ensure that data is erased or rectified without delay.

Principle (e): Storage Limitation

- All special category data processed by the Council for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in Retention Procedure. This retention procedure is reviewed regularly and updated when necessary.

Principle (f): Integrity and Confidentiality (Security)

The Council ensures that all electronic and physical information is processed within secure environments and protected through appropriate access and security controls.

Electronic systems and physical storage

- Access to information is restricted strictly on a need-to-know basis, with permissions applied according to role and operational requirement.
- Electronic information is stored within password-protected systems, supported by secure network infrastructure and monitored access controls.
- Physical records are stored in locked, access-controlled locations, ensuring confidentiality and preventing unauthorised handling.

Information security measures

The Council implements a range of security controls designed to maintain the integrity and confidentiality of information, including:

- User access control – ensuring only authorised individuals can access systems, data, and applications.
- Device security – requiring secure configuration, password protection, and up-to-date security patches on all devices used to access Council information.
- Secure disposal – ensuring electronic and physical information is destroyed using approved, secure methods.
- Breach reporting procedures – requiring all suspected or actual security incidents to be reported immediately in line with Council protocols.

All controls are reviewed periodically to ensure they remain effective, compliant with legislation and aligned with best practice guidance.

This policy should be read in conjunction with the Councils:

- Data Protection Policy
- Document Management Schedule
- Privacy Notice