Data Protection Policy

Owner	John Harrison, Town Clerk
Reviewer	Emily Hastings, Corporate Services Manager
Previous versions	
Templates used/adapted	
Approver	Full Council
Date approved	28.01.26
Resolution number	HTC/26/4/202
Next Review Due:	1 year or earlier in the event of legislative changes
Review date:	Jan 27
Related policies/procedures	Data Transparency, Freedom of Information & Publication Scheme I.T. Policy Retention and Erasure Policy CCTV policy *All policies should be read in conjunction with other policies where appropriate.*
Policy covers	All HTC
Revisions	

Contents

If you require any support in understanding or applying this policy, please contact the Corporate Services Manager. In addition, in line with the Equality Act 2010, we will make reasonable adjustments to remove or reduce disadvantages faced by disabled employees, Councillors, or applicants.

Policy statement and purpose

1. Hailsham Town Council is committed to processing personal data lawfully, fairly, transparently and securely.

2. This policy follows the UK GDPR and the Data Protection Act 2018, including rules for special category and criminal-offence data.

3. This policy sets out the Council's governance, controls and accountabilities for personal data processed in the delivery of council services and functions.

Scope

4. This policy applies to all councillors, employees, temporary staff, volunteers, and contractors who access or process personal data on behalf of the Council, whether in council systems (e.g., Microsoft 365) or approved third-party systems used under contract. It covers all formats (digital, paper, audio/video).

Legal and standards framework

5. UK GDPR and DPA 2018 (including special category and criminal offence data rules and Schedule 1 conditions), Information Commissioner's Officer (ICO) Accountability Framework, Data (Use and Access) Act 2025, Freedom of Information Act 2000, Public Sector Bodies (Websites and Mobile Applications), Accessibility Regulations 2018, Web Content Accessibility Guidelines (WCAG) 2.2 AA for web accessibility.

Roles and responsibilities

6. **Controller:** Hailsham Town Council.

7. **Contact:** Clerk/Proper Officer, Hailsham Town Council, enquiries@hailsham-tc.gov.uk, 01323 841702.

8. All councillors/staff/volunteers: must complete training, follow this policy and related procedures, and promptly report incidents/breaches.

9. Processors/Contractors: must meet the Council's data processing terms and security standards (see Sections 11 and 12).

The data protection principles and how the council meets them

10. **Lawfulness, fairness, transparency:** maintains an Article 30 Record of Processing (ROPA) and publishes privacy notices for core services.

11. **Purpose limitation:** Purposes are recorded per business area.

12. **Collecting only the information the Council actually needs:** Only information strictly necessary is collected; special category/criminal offence data is limited and supported by an data protection impact assessment (DPIA).

13. **Accuracy:** The Council will review key data regularly for accuracy.

14. **Storage limitation:** Retention follows the Council's schedule see Records Retention & Erasure Policy.

15. **Integrity & confidentiality (security):** role-based access, encryption, physical controls and restricted folders for sensitive data.

16. **Accountability:** Documented policies/procedures, training, DPIAs for higher-risk processing

Assertion 10 – the Council's commitments

17. Council-owned email/domain: all official correspondence uses @hailsham-tc.gov.uk accounts (no personal/free webmail). Generic addresses (e.g., Clerk@) are maintained.

18. Accessible website: the Council will keep its website compliant with WCAG 2.2 AA, has an up-to-date Accessibility Statement, and publish FOI/Transparency Code documents.

19. Policies & IT governance: maintains this Data Protection Policy, an Information Technology Policy, Records Retention & Erasure Policy, FOI/SAR Policy and Social Media/Communications Policy.

20. Data protection compliance: Maintain an up-to-date ROPA/data map, conduct DPIAs where required, and ensures regular training for staff and councillors.

The Council's processing of data – where your data is used

21. The Council processes personal data in the following areas:

22. Corporate Services personal data includes agendas/minutes (may capture political opinions), consultations, complaints, electoral roll copies (Wealden District Council is the controller), visitor sign-in.

23. Communications personal data includes images with consent; social media interactions; newsletters/mailing lists (consent-based).

24. Finance personal data includes payroll, pension administration, and information about suppliers and contractors.

25. Human Resources personal data includes recruitment (short-term retention for unsuccessful candidates), personnel records (sickness, occupational health, ID photos, next-of-kin), training records, DBS checks.

26. Operations & Facilities personal data includes H&S incident/accident reports, insurance claims, CCTV in buildings, risk assessments, access control logs, market holder information, allotments, leases/tenancies, burial records.

27. Youth Service personal data includes safeguarding (restricted), medical/consent information, attendance, supervision notes, youth programme communications, CCTV at venues.

28. James West Community Centre personal data includes room bookings and payments.

29. Post Office/Banking Hub personal data includes anti-money laundering/know your customer identification, postal proofs, transaction records (primarily in Post Office/Banking Hub systems), CCTV.

30. I.T personal data included within email, SharePoint/OneDrive/Teams.

31. Details of the purposes, data types, recipients, retention and lawful bases are recorded in the Council's data mapping/ROPA and service-specific DPIAs.

Individual rights and how to exercise them

32. You have the rights of access, rectification, erasure, restriction, objection, portability, and to withdraw consent (where applicable), and to complain to the ICO. For ICO complaints: https://ico.org.uk/make-a-complaint/.

33. Requests should be sent to enquiries@hailsham-tc.gov.uk (subject line: 'Data protection request').

34. The Council will verify identity, respond within statutory timeframes, and maintain a log of requests.

Records management, retention and erasure

35. Retention periods are recorded in the Retention & Erasure policy/schedule and within the data map. Where law requires longer retention (e.g., burial registers permanent), the Council complies; otherwise, data is deleted/anonymised when the purpose ends.

Security and IT/cyber controls

36. Microsoft 365: role-based access, access limited to authorised staff/councillors and administrators (Microsoft 365/and I.T. provider as processors).

37. Physical security: secure and controlled storage of sensitive material.

38. CCTV: signage, limited retention, access controls, incident downloads only when justified; Sussex Police is controller for town CCTV scheme (see CCTV policy).

39. Acceptable use/own devices: councillors and staff must use council email accounts, this ensures data is kept secure and helps us meet audit requirements and FOI/SAR requests; personal devices used for council business must meet the Council's security standards. E.g. e.g. secure email and storage.

Processors (external organisations/contractors who handle data for the Council) and data sharing

40. The Council only engages processors with appropriate safeguards.

41. Data sharing with public bodies occurs where lawful and necessary.

42. Processor links/records are maintained in the Council's data map.

International transfers

43. Where possible, the Council will keep data within the UK or EEA. Where vendors/platforms may involve restricted transfers, the Council ensures appropriate transfer mechanisms and safeguards (e.g., Microsoft's EU Data Boundary).

Personal data breaches

44. All staff/councillors must report suspected/actual breaches immediately to the Clerk.

45. The Council will investigate, mitigate harm, document outcomes, and notify the ICO within 72 hours where required (and affected individuals when risk is high).

46. Evidence of incidents and learning is retained.

Training and awareness

47. Induction and periodic (every 2 years) training is mandatory for staff and councillors, with records kept.

48. Targeted refreshers follow incidents, policy changes, or DPIA outcomes.