North Kent Marshes WLMB

Data Protection Policy

Approval date: 01/04/2026	Approved by: Board
Applies to: Board Members, officers and employees of the Board, and any contractors, consultants or agents who process personal data on behalf of the Board.	**Linked Documents:** Data Retention and Disposal Policy | CCTV Use and Privacy Statement | Information Systems and Security Policy.
Frequency of review: 3 years	**Next review date: April 2029**

1. Background

1.1 This policy sets out how the Board complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which together govern the lawful collection, use, and protection of personal data in the UK.

1.2 The Board also recognises its duties under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, which govern access to certain types of non-personal information.

1.3 The UK GDPR 2018 is designed to cover the collecting, storing, processing, and distribution of personal data. It applies to all individuals, whether they are an employee, elected member, or member of the public, and gives rights to individuals about what information is recorded.

1.4 This policy applies to all employees, members, volunteers, contractors, and those instructed by the Board to provide a service or those with whom the Board has entered into a joint working arrangement. This policy should be read alongside the Board's Data Retention and Disposal Policy, Information Security and Systems Policy, Privacy Notices, and Data Protection Procedures, which include guidance on breaches and subject access.

1.5 All employees have a responsibility for the information they generate, manage, transmit and use in line with the DPA and GDPR. It is their contractual duty to secure personal and confidential data at all times. Any person who knows or suspects that a breach of data security has occurred should report the breach immediately in accordance with this policy.

1.6 Notifying the Information Commissioners Office (ICO) of a personal data breach must be done without delay where feasible and no later than 72 hours of becoming aware of a breach. If the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals affected without undue delay.

North Kent Marshes WLMB

Data Protection Policy

2. Purpose

2.1 This policy applies to all personal data held by the Board, whether in digital or physical form, and to all staff, members, contractors, and service providers handling data on the Board's behalf. The purpose of this policy is to ensure that the provisions of the DPA and the GDPR are complied with and to protect the personal data of individuals. The data protection principles and GDPR regulations are set out in section 3 of this policy.

2.2 This policy aims to assist the Board in meeting the relevant data protection obligations under the appropriate legislation. It is the responsibility of all employees, members, and any person holding or processing personal data on behalf of the Board to assist with the implementation of this policy.

3. Data Protection Principles and General Data Protection Regulation Responsibilities

3.1 To meet the requirements of the UK General Data Protection Regulation and the Data Protection Act 2018, the Board fully endorses the data protection principles, including:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

3.2 To meet the requirements of the General Data Protection Regulation 2018, the Board fully endorses the main responsibilities as set out in Article 5, adhering to them at all times. Data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay ('accuracy');

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

4. Data Handling

4.1 The Board complies with the DPA principles and the GDPR responsibilities when handling personal data. Individuals have rights within the legislation which includes a certain control over how their information is handled. The Board will:

- Observe fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information and only to the extent that it is required to fulfil operational needs or comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that information held is erased at the appropriate time in line with the Data Retention and Disposal Policy.
- Ensure that the rights of individuals about whom we hold information can be exercised fully under the DPA and GDPR including;
  - The right to be informed that processing is being undertaken.
  - The right of access to their personal information (a Subject Access Request).
  - The right to correct and/or rectify if the data is incorrect.
  - Request erasure or restriction of processing ("the right to be forgotten").
  - The right to data portability (transfer of data from one Data Controller to another).
- Ensure an appointed Data Protection Officer is in place who is the point of contact for any Data Protection or Personal Data, processing and/or queries.
- Take appropriate technical and organisational security measures to safeguard personal information (new projects include Data Impact Assessment where appropriate).
- Ensure that all employees are trained and supervised appropriately to handle personal information if their role requires personal data handling.
- Process requests for access to personal information in a timely and courteous manner, if the request is refused, the Board will state why and supply the information necessary should be requestor wish to complain.

- Record any breaches in data protection and report any which are likely to result in a risk to the rights and freedoms of individuals to the ICO within 72 hours of the Board becoming aware of the breach, where the breach is likely to result in a high risk to individuals, those individuals are to be notified with immediate effect.
- Periodically review the management of personal information and update the relevant policies and procedures accordingly.

5. Confidentiality, Security, and Reporting a Data Breach

5.1 For full operational guidance, see the Board's Data Protection Procedures, which detail breach notification and investigation processes.

5.2 Employees must not access, copy, alter, interfere with, or disclose personal data held by the Board unless permitted to do so by under data protection laws. Failure to follow the rules set out in this policy could lead to disciplinary action or even a personal prosecution.

5.3 Individuals that process personal data must not comply with the Board's information Security ICT Use policy to safeguard personal data.

5.4 Any employee, member or other person who becomes aware of a weakness in the Board's data protection procedures or who becomes aware of any breach of the policy should report the concern to their line manager at the earliest opportunity and to the Data Protection Officer without delay, who will refer to the Data Breach Procedures.

5.5 Where there has been a data breach, or potential data breach, the Board has a duty to find out what data has been lost or stolen, to mitigate the loss and to take steps to notify persons affected where appropriate. An incident or anticipated incident must be reported immediately to the Data Protection Officer in accordance with the Board's Data Breach Procedures. When reporting an incident, use the Data Breach Questionnaire at Appendix A of the Data Breach Notification Procedure. The DPO will investigate any such breach in accordance with the Data Breach Procedures.

6. Further Information

6.1 The Board is registered with the Information Commissioner's Office (ICO) and pays an annual fee.

6.2 The Board adheres to the Data Retention and Disposal Policy, providing details of the periods for which documents are held.

6.3 The Board has a privacy policy which can be found on the website.

6.4 Queries, issues, and complaints about where personal information is, or has been processed, should be directed to the Data Protection Officer in the first instance.

6.5 Failure by employees to fully comply with this policy may lead to disciplinary action being taken against them. For serious breaches, this could also result in personal criminal liability and therefore prosecution.

6.6 Failure by Board members to fully comply with this policy is likely to constitute a breach of the Members' Code of Conduct, which means that they may be expected to resign, and for serious breaches, this could also result in personal criminal liability and therefore prosecution.

6.7 The Board maintains separate Privacy Notices for members of the public (published on the website) and for employees, contractors, and Board members. These outline how personal data is collected, used, stored, and shared.

7. Access to personal information

7.1 Individuals have the right to request access to their personal data under the UK General Data Protection Regulation. This is known as a Subject Access Request (SAR). Requests can be made in writing or verbally and should be directed to the Data Protection Officer:

Clerk and Engineer - Data Protection Officer
Unit 13, Conqueror Court, Vellum Drive
Sittingbourne, ME10 5BH
enquiries@northkentwlmb.org.uk

7.2 The Board has an internal procedure for handling SARs to ensure that requests are processed lawfully and within the required timescales. This procedure is available to staff and Board members on request.

Version Control

Version	Date Approved	Summary of Changes
1.0	01/04/2026	Initial policy approved