BEDFORD GROUP OF DRAINAGE BOARDS

DATA PROTECTION POLICY

GOVERNANCE

Last review date: April 2022

To be reviewed every 5 years

Next review date: April 2027

Reviewed by: Joint Management Committee

Adopted by:

Alconbury & Ellington Internal Drainage Board
Bedfordshire & River Ivel Internal Drainage Board
Buckingham & River Ouzel Internal Drainage Board

The Data Protection Act 2018 and the General Data Protection Regulation 2018 are designed to cover the collecting, storing, processing and distribution of personal data. It gives rights to individuals about whom information is recorded and maintained. This applies to all individuals whether they are employees, Board members, ratepayers, customers, suppliers, or members of the public. This policy sets out how the Bedford Group Member Boards will ensure that your personal data is protected.

Contents

1. INTRODUCTION

(a) The Data Protection Act 2018 (DPA) came into force on 25 May 2018 replacing the Data Protection Act 1998. The General Data Protection Regulation 2018 (GDPR) is the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR was adopted in the UK on 14 April 2016, came fully into force on 25 May 2018 and is to be adhered to, alongside the Data Protection Act 2018.

(b) The General Data Protection Regulation 2018 is designed to cover the collecting, storing, processing and distribution of personal data. It gives rights to individuals about what information is recorded. This applies to all individuals whether they are an employee, elected member or a member of the public.

(c) 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 along with the Document Retention and Destruction Policy, Information Security and Systems Acceptable Use Policy and Data Breach Procedures provide information and guidance to support each Board's work and activities when dealing with personal information.

(d) 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.

(e) 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. In the event that 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.

2. PURPOSE

(a) 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.

(b) This policy aims to assist each Member Board and other relevant persons in meeting their data protection obligations under the GDPR and related data protection legislation. It is the responsibility of all employees, members and any person holding or processing personal data on behalf of each Member Board to assist with the implementation of this policy.

3. DATA PROTECTION PRINCIPLES & GENERAL DATA PROTECTION REGULATION RESPONSIBILITIES

(a) To meet the requirements of the Data Protection Act 2018, each Board fully endorses the eight principles contained therein, adhering to them at all times. This legislation governs the processing of personal information both by way of manual records and computerised information, including CCTV.

(b) The eight Data Protection principles:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any way incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

(c) 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;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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; and

- 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.

4. DATA HANDLING

(a) Each Member 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. Each 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 to comply with any legal requirements;
- ensure the quality of information used;
- ensure that information held is erased at the appropriate time inline with the Group's Document Retention & Destruction policy;
- ensure that the rights of individuals about whom we hold information can be exercised fully under the DPA & 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
  - Block or erase information that is regarded as wrong ("the right to be forgotten")
  - The right to data portability (transfer of data from one Data Controller to another)
- have an appointed Data Protection Officer 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 a Data Impact Assessment where appropriate);
- ensure that personal information is not transferred abroad without suitable safeguards;
- 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 the 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

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

(b) Individuals that process personal data must comply with the Group's Information Security ICT Use policy to safeguard personal data.

(c) Any employee, member or other person who becomes aware of a weakness in the Group'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.

(d) Where there has been a data breach, or potential data breach each Member 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 DPO, in accordance with the Group's Data Breach Procedures. When reporting an incident please fill in the Data Breach Questionnaire in Appendix A of this policy. The DPO will investigate any such breach in accordance with the Data Breach Procedures.

6. FURTHER INFORMATION

(a) Each Member Board is registered with the Information Commissioners Office (ICO) and pays an annual fee.

(b) Each Board adheres to the Document Retention & Destruction policy providing details of the periods for which documents are held.

(c) Each Board has a Privacy Policy which can be found on the web-site and/or supplied upon request.

(d) Where a person wishes to raise a query, issue or complaint about how their personal information is, or has been, processed, they should, in the first instance be directed to the data protection officer (see details below).

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

(f) 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.

7. ACCESS TO PERSONAL INFORMATION

(a) For information about how to request access to personal information please contact:

Data Protection Officer
Vale House
Broadmead Road
Stewartby
Bedfordshire
MK43 9ND

Tel: 01234 767995
contact@idbs.org.uk

A SMITH
DATA PROTECTION OFFICER

Version Control

Version	Changes made	Date
Version 1	n/a	April 2022

Appendix A: Data Breach Questionnaire

Please answer the questions below; enter N/A if the question is not relevant or TBC (to be confirmed) if the question cannot be answered at present.

If you can identify someone else who may be able to answer any of the questions please indicate this in your response.

Send the completed form to the Data Protection Officer at contact@idbs.org.uk You will be advised on further actions. If the breach is currently ongoing (i.e. data is still at risk or exposed), contact 01234 767995 as soon as possible.

Date:	Your Name:	Contact: Email / Mobile

	Your answer	DPO notes
About the data breach		
When did this data breach occur?		
When did the IDB become aware of the data breach?		
How did you become aware of the breach?		
What do you think caused the breach? (e.g. human error, theft, cyber-attack)		
Where did this data breach occur?		
Please provide a brief description of the circumstances leading to the breach		
About the data		
Who would normally be responsible for the data?		
Does any of the data relate to identifiable living individuals?		
What does the data consist of? Please provide a full description		
Were any of the following data types involved (if yes, tick all boxes that apply) * × Includes any inherited or acquired data which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question.	☐ Racial or ethnic origin ☐ Political opinions ☐ Religious beliefs ☐ Trade union membership ☐ Health data/medical data (physical or mental), well-being etc.	

	Your answer	**DPO notes**
† Any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, fingerprints, blood samples etc. ‡ Includes employment rates, crime rates, poverty status, education levels, life expectancy etc. ◊ Includes CVs, job application forms, job references, PDRs, development reviews, pension, payroll, sickness etc.	☐ Sexual life/orientation data Criminal offences ☐ Detail of proceedings relating to criminal offences ☐ Genetic data × ☐ Biometric data † ☐ Socio Economic Data ‡ ☐ Grades/Achievements/Personal Statements etc. ☐ Financial data, including account numbers, card details etc. ☐ Employment data ◊ ☐ None of the above	
Does this incident/breach involve Commercially Sensitive Data? *	Yes ○ No If yes, what was the classification? * ☐ Public ☐ Protected ☐ Restricted ☐ Reserved ☐ None of the above	
Approximately how many individuals are affected?		
Was the data secured against unauthorised access? If so, can you describe how it was secured? E.g. Was the data encrypted? Who held the encryption keys? How were the encryptions keys kept secure?		
Do you know if anyone has had access to the data when it was no longer under your control? Please explain who might have been able to access the data		

	Your answer	DPO notes
Do you have a copy of the data that was lost?		
Have the staff involved in this data loss received Data Protection training, and if so, when?		
Actions since breach*		
Have you attempted to get the data back from those who now hold it?		
Have you informed the data subjects that this incident has occurred?		
Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so, please provide brief details.		
Are you carrying out an internal investigation into the incident – If so when will you complete it and what format will it take?		
Have you informed any other regulatory body of the matter? If so, please provide their details and an outline of their response.		
What actions have you taken to prevent similar incidents in the future?		
Is there any other information you feel would be helpful to an assessment of the incident?		