Bedford Group of Drainage Boards (Bedfordshire & River Ivel IDB, Buckingham & River Ouzel IDB and Alconbury & Ellington IDB)

Data Protection Policy

1 INTRODUCTION

1.1 This Policy sets out the obligations of the Bedfordshire & River Ivel IDB, Buckingham & River Ouzel IDB and Alconbury & Ellington IDB (the Boards) regarding data protection and the rights of staff, clients, assignees, business contacts ("data subjects") in respect of their personal data under the General Data Protection Regulation 2016 (GDPR), the regulation, and the General Data Protection Act 2018.

1.2 The Boards are data controllers and processors. The GDPR applies to controllers and processors and applies to personal data, meaning any information relating to an identifiable person who can be directly or indirectly identified, by reference to an identifier, and sensitive personal data.

Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The only category that applies to the Boards could be in relation to the collection of Trade Union subscriptions and data relating to health from sick notes and occupational health.

2 LAWFUL BASIS FOR PROCESSING

2.1 The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998. However, the GDPR places more emphasis on being accountable for and transparent about the Boards' lawful basis for processing.

2.2 The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. The Boards now needs to review existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as our existing condition for processing.

2.3 The biggest change is for public authorities, such as the Boards, who now need to consider the new 'public task' basis first for most of their processing and have more limited scope to rely on consent or legitimate interests.

2.4 The Boards will be in breach of the GDPR if we do not clearly identify the appropriate lawful basis (or bases, if more than one applies).

2.5 The GDPR brings in new accountability and transparency requirements. The Boards should therefore make sure it clearly documents the lawful basis so that it can demonstrate its compliance in line with Articles 5(2) and 24.

2.6 The Boards must now inform people upfront about the lawful basis for processing their personal data. The Boards need therefore, to communicate this information to individuals and ensure it is included in all privacy notices.

2.7 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) **Consent**: the individual has given clear consent for the Boards to process their personal data for a specific purpose.
(b) **Contract:** the processing is necessary for a contract the Boards have with the individual, or because they have asked the Boards to take specific steps before entering into a contract.
(c) **Legal obligation:** the processing is necessary for the Boards to comply with the law (not including contractual obligations).
(d) **Vital interests:** the processing is necessary to protect someone's life.
(e) **Public task:** the processing is necessary for the Boards to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) **Legitimate interests:** the processing is necessary for the Boards' legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

A register of data types held and the lawful basis to process this data is shown in the table below.

3 INDIVIDUAL RIGHTS

3.1 The GDPR provides the following rights for individuals:

(a) **The right to be informed**
Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The Boards achieve this by publishing their Privacy Notices.

(b) **The right of access**
Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

(c) **The right to rectification**
The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

(d) **The right to erasure**

The GDPR introduces a right for individuals to have personal data erased.
The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The right is not absolute and only applies in certain circumstances. For example, it does not apply for the performance of a task carried out in the public interest or in the exercise of official authority.

(e) **The right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing.

(f) **The right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

(g) **The right to object**

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

(h) **Rights in relation to automated decision making and profiling.**

The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. The GDPR applies to all automated individual decision-making and profiling.

4 ACCOUNTABILITY AND GOVERNANCE

4.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. We are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the Information Commissioner's Office (ICO) has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances. Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

4.2 **Documentation**

The GDPR contains explicit provisions about documenting the Boards' processing activities. We must maintain records on several things such as processing purposes, data sharing and retention. A register can be found in the table below.

The Boards may be required to make the records available to the ICO on request. Records must be kept in writing. Records must be kept up to date and reflect our current processing activities.

4.3 **Data protection by design and default**

Under the GDPR, the Boards have a general obligation to implement technical and organisational measures to show that the Boards have considered and integrated data protection into the Boards' processing activities. Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.

4.4 **Data protection impact assessments**

A data protection impact assessment (DPIA) is a process to help the Boards identify and minimise the data protection risks of a project. The Boards must do a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data. To assess the level of risk, the Boards must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

This is not likely to apply to the Boards but should be borne in mind.

4.5 **Data Protection Officer**

The GDPR introduces a duty for the Boards to appoint a data protection officer (DPO) as we are public authorities. DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (in the UK the supervisory authority is the ICO).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. A DPO can be an existing employee or externally appointed.

Alice Smith, Executive Assistant at the Boards' offices, is appointed as the Boards' Data Protection Officer.

4.6 **Security**

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

4.7 **Personal data breaches**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Boards must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Boards must also inform those individuals without undue delay.

The Boards should ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. The Boards must also keep a record of any personal data breaches, regardless of whether you are required to notify.

4.8 **Children**

It is not envisaged that the personal details of children will be processed and the DPO should be consulted if this becomes a requirement.

5 DATA PROTECTION PRINCIPLES

5.1 The Boards fully endorse the eight data protection principles, adhering to them at all times.

These principles are:

(a) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
(b) 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.
(c) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
(d) Personal data shall be accurate and where necessary, kept up to date.
(e) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
(f) Personal data shall be processed in accordance with the rights of data subjects under the GDPR.
(g) 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.
(h) 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.

5.2 **The Boards' commitment to the Data Protection Principles**

The Boards will do the following to comply with the principles:

(a) Observe fully the conditions regarding the fair collection and use of information.
(b) Meet their legal obligations to specify the purposes for which information is used.
(c) 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.
(d) Ensure the quality of information used.
(e) Ensure that information held is erased at the appropriate time.
(f) Ensure that the rights of individuals about whom we hold information can be exercised fully under GDPR.
(g) Appropriate technical and organisational security measures to safeguard personal information.
(h) Ensure that personal information is not transferred abroad without suitable safeguards.

5.3 **The Boards adhere to their commitment to Data Protection by:**

(a) Allocation of specific responsibility for data protection to at least one person known as the Data Protection Officer.
(b) Ensure that employees handling personal information are supervised appropriately.
(c) Requests for access to an individual's own personal information are dealt with in a timely and courteous manner.
(d) Record any incidents of breach in data protection policy and keep a register.
(e) Undertake regular review of management of personal information and update when necessary.

5.4 **Access to Personal Information**

For information about how to request subject access to personal information please contact: contact@idbs.org.uk

Revised:	October 2019	
Date of JMC approval:	14 October 2019	
Date of Board approval:	Buckingham and River Ouzel -	5 November 2019
	Bedfordshire and River Ivel-	7 June 2021
	Alconbury and Ellington –	5 May 2020

Article 30 Record of Processing Activities

Data controller

Name: **Bedford Group of IDBs (Bedfordshire & River Ivel IDB, Buckingham & River Ouzel IDB and Alconbury & Ellington IDB)**

Address: Vale House, Broadmead Road, Stewartby, Bedford MK43 9ND

Telephone: 01234 767995 **Email:** contact@idbs.org.uk

Data Protection Officer		**Senior Information Risk Officer**	
Name:	Ruth Easom	**Name:**	Frances Bowler
Email:	ruth.easom@idbs.org.uk	**Email:**	frances.bowler@idbs.org.uk

Business function (Individual Board)	**Business function (Bedford Group)**	**Purpose of processing**	**Name of joint controller (if applicable)**	**Categories of individuals**	**Categories of personal data**	**Categories of recipients**	**General description of technical and organisational security measures (if possible)**	**Article 6 Lawful basis for processing personal data**	**Article 9 basis for processing special category data**
Rating		Rating records	N/A	Ratepayers	Contact details	Public (Electoral Register)	Encrypted Storage/Access Controls	Article 6(1)(e) - Public task	
Planning & Consenting		Planning Consultation	District Coucils, Borough Councils and Unitary Authorities within Board area	Public	Contact details	District Councils, Borough Councils and Unitary Authorities	Encrypted Storage/Access Controls	Article 6(1)(e) - Public task	
Planning & Consenting		Consent Application		Applicant	Contact details	N/A	Encrypted Storage/Access Controls	Article 6(1)(e) - Public task	
	Planning & Consenting	Consents Application in extended area (LLFAs)	Central Beds BC, Milton Keynes Council, Northants Council	Applicant	Contact detalis	N/A	Encrypted Storage/Access Controls	Article 6(1)(e) - Public task	
Finance (B&I Board)	Finance	Payroll	N/A	Employees	Contact, bank, pension and tax details	HMRC	Encrypted Storage/Access Controls	Article 6(1)(c) - Legal obligation	
Finance	Finance	Sales	N/A	Customers	Contact details	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	
Finance	Finance	Purchase	N/A	Suppliers	Contact and bank details	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	
Human Resources (B&I Board)		Personel file	N/A	Employees	Contact, emergency contact, pay and annual leave details	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	

Business function (Individual Board)	Business function (Bedford Group)	Purpose of processing	Name of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	General description of technical and organisational security measures (if possible)	Article 6 Lawful basis for processing personal data	Article 9 basis for processing special category data
Human Resources (B&I Board)		Personel file	N/A	Employees	Sick leave details	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	Article 9(2)(b) - Employment
Human Resources (B&I Board)		Personel file	N/A	Employees	Performance details	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	
Human Resources (B&I Board)		Personel file	N/A	Employees	Driver declarations	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	Article 9(2)(b) - Employment
Human Resources (B&I Board)		Personel file	N/A	Employees	Occupational Health	N/A	Encrypted Storage/Access Controls	Article 6(1)(b) - Contract	Article 9(2)(b) - Employment
Admin		Board Functions	N/A	Board Members	Contact details, Register of Members Interest	N/A	Encrypted Storage/Access Controls	Article 6(1)(e) - Public task	