Black Sluice Internal Drainage Board
Policy No: 32
Data Protection Policy

Review Dates:

Original Issue	16th January 2013
Board Approved	30th May 2018

1 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018. Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so as we are complying properly with the current law then most of our approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so we will have to do some things for the first time and some things differently.

1.2 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 in particular by reference to an identifier, and sensitive personal data.

1.3 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 Black Sluice IDB is 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 Board's 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 Board now needs to review our existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing condition for processing.

2.3 The biggest change is for public authorities, such as the Board, 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 We can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. Once the GDPR is in effect, it will be much harder to swap between lawful bases if the Board finds that our original basis was invalid. The Board will be in breach of the GDPR if we do not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

2.5 The GDPR brings in new accountability and transparency requirements. The Board 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 Board must now inform people upfront about the lawful basis for processing their personal data. The Board needs therefore, to communicate this information to individuals by 25 May 2018, and ensure that you include it in all future 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 Board to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract the Board has have with the individual, or because they have asked the Board to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for the Board 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 Board 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 at Appendix 1.

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 board achieves this by publishing the Privacy Notice at appendix 2.

(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. Details of how to object are included in our Privacy Notice at appendix 2.

(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 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 Board's processing activities. We must maintain records on several things such as processing purposes, data sharing and retention. A register can be found at appendix 1.

The Board 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 Board has a general obligation to implement technical and organisational measures to show that the Board has 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 Board identify and minimise the data protection risks of a project. The Board 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 Board 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 Board but should be borne in mind.

4.5 **Data Protection Officer**

The GDPR introduces a duty for the Board to appoint a data protection officer (DPO) as we are a public authority. 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.

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.

Daniel Withnall MCGI MInstLM FMAAT, Finance Manager and Responsible Financial Officer, is appointed at 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 Board 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 Board must also inform those individuals without undue delay.

The Board 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 Board 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 Black Sluice Internal Drainage Board fully endorses 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 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 **Black Sluice Internal Drainage Board's commitment to the Data Protection Principles**

Black Sluice Internal Drainage Board will do the following to comply with the principles:

(a) Observe fully the conditions regarding the fair collection and use of information.
(b) Meet its 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) Take appropriate technical and organisational security measures to safeguard personal information.
(h) Ensure that personal information is not transferred abroad without suitable safeguards.

5.3 **Black Sluice Internal Drainage Board adheres to its 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: mailbox@blacksluiceidb.gov.uk

Controller			
Name and contact details		**Data Protection Officer (if applicable)**	
Name	Black Sluice Internal Drainage Board	**Name**	Daniel Withnall
Address	Station Road, Swineshead, Boston, Lincolnshire, PE20 3PW	**Address**	Black Sluice IDB, Station Road, Swineshead, Boston, Lincolnshire. PE20 3PW
Email	mailbox@blacksluiceidb.gov.uk	**Email**	Daniel.Withnall@Blacksluiceidb.gov.uk
Telephone	01205 821440	**Telephone**	01205 821440

Article 6(1)(a) - Consent	Article 9(2)(a) - Consent
Article 6(1)(b) - Contract	Article 9(2)(b) - employment
Article 6(1)(c) - legal obligation	
Article 6(1)(d) - Vital Interests	
Article 6(1)(e) - Public Task	
Article 6(1)(f) - Legitimate Interests	

Article 30 Record of Processing Activities

Business function	Purpose of processing	Name and contact details 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)		Article 6(1)(e) - Public Task	
Planning & Consenting	Planning Consultation	Boston Borough Council	Public	Contact Details	District/Borough Council	Encrypted storage and transfer	Article 6(1)(e) - Public Task	
Planning & Consenting	Planning Consultation	South Holland District Council	Public	Contact Details	District/Borough Council	Encrypted storage	Article 6(1)(e) - Public Task	
Planning & Consenting	Planning Consultation	North Kesteven District Council	Public	Contact Details	District/Borough Council	Encrypted storage	Article 6(1)(e) - Public Task	
Planning & Consenting	Planning Consultation	South Kesteven District Council	Public	Contact Details	District/Borough Council	Encrypted storage	Article 6(1)(e) - Public Task	
Planning & Consenting	Planning Consultation	Lincolnshire County Council	Public	Contact Details	County Council	Encrypted storage	Article 6(1)(e) - Public Task	
Planning & Consenting	Consent Application	N/A	Applicant	Contact Details	N/A	Encrypted storage	Article 6(1)(e) - Public Task	
Planning & Consenting	Consent Application in extended Area	Lincolnshire County Council	Applicant	Contact Details	N/A	Encrypted storage	Article 6(1)(e) - Public Task	
Finance	Payroll	N/A	Employees	Contact details	HMRC	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	
Finance	Payroll	N/A	Employees	Bank details	HMRC	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	
Finance	Payroll	N/A	Employees	Pension details	HMRC	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	
Finance	Payroll	N/A	Employees	Tax details	HMRC	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	
Finance	Sales	N/A	Customers	Contact details	N/A	Encrypted storage	Article 6(1)(b) - contract	
Finance	Purchase	N/A	Suppliers	Contact details	N/A	Encrypted storage	Article 6(1)(b) - contract	
Finance	Purchase	N/A	Suppliers	Bank details	N/A	Encrypted storage	Article 6(1)(b) - contract	
Human Resources	Personel file	N/A	Employees	Contact details	N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	
Human Resources	Personel file	N/A	Employees	Pay details	N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	
Human Resources	Personel file	N/A	Employees	Annual leave details	N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	
Human Resources	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	Personel file	N/A	Employees	Performance details	N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	
Human Resources	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	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	N/A	Encrypted storage	Article 6(1)(e) - Public Task	
Admin	Board Functions	N/A	Co-Opted Board Members	Contact Details	N/A	Encrypted storage	Article 6(1)(a) - Consent	

Black Sluice
Internal Drainage Board

Station Road
Swineshead
Boston
Lincolnshire
PE20 3PW

01205 821440

www.blacksluiceidb.gov.uk

mailbox@blacksluiceidb.gov.uk

PRIVACY NOTICE

At Black Sluice Internal Drainage Board, we're committed to protecting and respecting your privacy.

This Notice explains when and why we collect personal information about people, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this Notice from time to time so please check occasionally to ensure that you're happy with any changes.

If you have any questions regarding this Notice and our privacy practices you can contact us using the details above.

Who are we?

The Black Sluice Internal Drainage Board is an authority set up to control water levels and reduce the risk of flooding within the Board's area. It operates 34 pumping stations and maintains 500 miles of watercourses within its area and has a policy of undertaking this work with regard to protecting and enhancing the environmental features in these watercourses.

Public Bodies dealing with drainage matters have a long history which stretches back to 1252, but most IDBs today were established by National Government following the passing of the Land Drainage Act 1930. The activities and responsibilities of the Boards are controlled by this and subsequent Land Drainage Acts, and other subordinate legislation.

How do we collect information from you?

In most cases information will be collected from you directly but the Board may, from time to time, use powers included in law to require information of others. The legal basis for obtaining this information will be assured and we will tell you how we obtained your personal information.

What type of information is collected from you?

The personal information we collect might include your name, contact details and details of any land you either own or occupy. If you make a payment to us using a card your card information is not held by us, it is collected by, or transmitted directly to in case of a phone payment, our third party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions. Cards details are never recorded or stored by Black Sluice IDB.

How is your information used?

We may use your information to:

(a) Carryout Drainage Board Functions as per the Land Drainage Act 1991.
(b) Process applications in relation to the Board's Byelaws.
(c) Process applications on behalf of Lincolnshire County Council, the lead local flood authority, under Section 23 of the Land Drainage Act 1991.
(d) Carry out our obligations arising from any contracts entered into by you and us.
(e) Process a job application.

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. We will hold your personal information on our systems for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

Who has access to your information?

We will not sell, rent or share your information with third parties for marketing purposes.

Third Party Service Providers working on our behalf: We may pass your information to our third party service providers, agents subcontractors and other associated organisations for the purposes of completing tasks and providing services to you on our behalf. However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure and not to use it for their own direct marketing purposes. Please be reassured that we will not release your information to third parties for them to use for their own direct marketing purposes, unless we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

When you are using our secure online payment pages, your payment is processed by a third party payment processor, who specialises in the secure online capture and processing of credit/debit card transactions. If you have any questions regarding secure transactions, please contact us.

How you can access and update your information

The accuracy of your information is important to us. If you change email address, or any of the other information we hold is inaccurate or out of date, please contact us using the details above.

Security precautions in place to protect the loss, misuse or alteration of your information

When you give us personal information, we take steps to ensure that it's treated securely. Any sensitive information is encrypted and protected.

Non-sensitive details (your email address etc.) transmitted normally over the Internet, can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems.

Review of this Notice

We keep this Notice under regular review. This Notice was last updated in April 2018.