Policy Ref - GOV 011

Document Retention and Document Privacy Policy

WITHAM AND HUMBER DRAINAGE BOARDS

A group of four independent statutory Land Drainage, water levels and Flood Risk Management Authorities working collectively under a partnership agreement in accordance with section 11(5) of the Land Drainage Act (1991).

Four Independent Boards:

- *Witham First District Internal Drainage Boards*
- *Witham Third District Internal Drainage Boards*
- *Upper Witham Internal Drainage Boards*
- *North East Lindsey Internal Drainage Boards*

Version: 01

Date of policy: December 2024

Review due on or before: December 2029

Date of Approval by Joint Services Committee (JSC) on behalf of North East Lindsey (NEL), Upper Witham (UW), Witham First District (W1) and Witham Third District (W3) IDBs: 09th December 2024

Author: Risk Manager

Policy Owner: Associate Director of Human Resources

Contents

1.0 - Introduction

The Board recognises the importance of maintaining the appropriate documents, in the appropriate manner and importantly destroying documents, if required to destroy, at the right time and in the right way.

Therefore, this Policy incorporates:

- Document Retention
- GDPR and Data Protection
- Freedom of Information (FOI)

1.1 - Purpose of these Policies

The purpose of these three policies is to ensure that from conception of the document/ information through the holding, and potential destruction of any document it is clear on timelines to ensure transparency and consistency throughout the Boards.

It is also important that any documents which are held, which include personal information are held appropriately.

The Board is clear that personal information does need to be held to ensure the Boards are able to fulfil their statutory functions, such as holding landowner, rate payer and information on enforcement as an example. It also recognises that employee information has to be held from onboarding and taking proof of the right to work in the UK, through to personal details to ensure that our employees are paid.

It is important that therefore, any information which may be requested by members of the Public is scrutinised to ensure that it is appropriate to share and therefore the FOI section of the policy provides the guidelines that the Board will follow for any such FOI requests.

1.2 – Equality, Diversity and Inclusion:

This policy aims to meet the requirements of the Equality Act 2010 and ensure that no employee receives less favourable treatment on the grounds of gender, sexual orientation, transgender, civil partnership/marital status, appearance, race, nationality, ethnic or national origins, religion/belief or no religion/belief, disability, age, carer, pregnancy or maternity, social status or trade union membership.

2.0 – Document Retention and Document Privacy Policy

2.1 – Document Retention Policy

Records and the data held are vital assets which require careful management to ensure the Boards can conduct their business, and comply with statutory requirements.

The purpose of the Document Retention Policy is to set out arrangements for record management, in terms of the storage and retention of data, and the archive and or destruction of such data.

2.1 - Introduction

The effective management of records and data in all formats depends as much on their efficient disposal as well as their long-term preservation. The untimely destruction of records may adversely affect service delivery but so will the unnecessary retention of outdated and potentially inaccurate records.

Disposal is necessary not only to reduce administrative burdens but also to ensure that information is not retained for longer than necessary and that accurate records are maintained for appropriate periods to satisfy applicable operational and legal requirements [e.g. particular HMRC timeline requirements on retention].

This policy details how the Board will comply with Data Protection Legislation (Section 2.2 and Freedom of Information Requests Section 2.3).

To achieve this the Boards will ensure held data is:

- adequate, relevant and not excessive.
- accurate and where necessary kept up to date.
- not kept for longer than is necessary for its purpose.

2.2 – Retention Periods

The Retention Schedule provides guidance to the length of time that records should be retained, irrespective of the media on which they are created or held including:

- Paper documents e, g., reports, leaflets, minutes, maps etc
- Electronic documents e.g., Office suite documents, webpages, emails, scanned maps and document etc.
- Photographs and recordings (in any type of format)

Retention periods are determined based upon the nature of the information held, not the medium in which it is maintained. For example, information which is held in electronic form should only be retained for the same period as it would be kept if it were in paper form.

It is not necessary to retain both paper and electronic versions of the same record, nor to retain duplicate copies of records. Retention arrangements for electronic records should ensure that they will remain complete, unaltered and accessible throughout the retention period.

The value of information tends to decline over time, so most records should only be retained for a limited period of time and eventually be destroyed. A recommended minimum retention period, derived from operational or requirements, is provided for each category of record and applies to all records within that category.

During their retention period, operational needs may require records to be held in different locations and on different media, but they should always be properly managed in accordance with this policy.

A small proportion of records which are of permanent historical significance will be preserved in the archives. The Chief Executive is responsible for the selection of records for permanent preservation and the maintenance of the archives.

No data file or record should be retained for more than six years after it is closed unless a good reason for longer retention can be demonstrated. It may well be appropriate having regard to the nature of the record to opt for a shorter period.

Reasons for longer retention will include the following:

- Statute requires retention for a longer period.
- The record contains information relevant to legal action which has been started or is in contemplation.
- Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.
- Records required to be archived for historical or research purposes, e.g. the record relates to an important policy development or relates to an event of local or national purpose.
- Records are maintained for the purpose of retrospective comparison.
- Records relate to individuals or providers of services who are judged unsatisfactory. The individuals may include employees who have been the subject of serious disciplinary action.

2.3 – Schedule of Contractual Records

Type	**Item**	**Description**	**Disposal (minimum period)**
Policy matters	1	Policy on contracts, normally contained in a separate registered file series	First and second review
Initial proposal	2	End user requirement	Six years
	3	List of approved suppliers	An active document – updated regularly
	4	Statements of interest	One year from date of last paper
	5	Draft specification	Destroy when specification has been agreed
	6	Agreed specification	Six years from the end of contract
	7	Evaluation criteria	
	8	Invitation to tender	
Tendering	9	Unsuccessful tender document	One year after date of last paper

	10	Successful tender document	Six years from award of contract
	11	Background information supplied by department	One year after date of last paper
	12	Interview panel – report and notes of proceedings	One year from end of contract
	13	Commissioning letter	One year from end of contract
	14	Signed contract	Six years from end of contract
Contract operation and monitoring	15	Reports from contractors	Two years from end of contract
	16	Schedules of works	Two years from end of contract
	17	Bills of quantity (building contracts)	Sixteen years
	18	Surveys and inspections a. equipment and supplies b. buildings	a. Two years from the date of last paper b. Second review
	19	Records of complaints	Six years from end of contract
	20	Disputes over payment	
	21	Final accounts	
	22	Minutes and papers of meetings	Second review
Amendments to contracts	23	Changes to requirements	Six years from end of contract
	24	Forms of variation	
	25	Extensions to contract	

If contractual records are associated with major policy developments in government departments, or significant funding it may be deemed pertinent to hold the documents for longer.

If the works for the project are pertinent to keep for evidence of maintenance and repair, demonstrate history which may be required in the future e.g., for major works to repair watercourses, pumping stations etc., these will be kept as long as required, which is likely to be longer than the minimum retention.

2.4 – Board and Legal Records

No.	Board and Legal Records	Disposal (minimum period)
1.	Articles of incorporation	Permanent
2.	Charter	Permanent
3.	By-Laws	Permanent
4.	Agenda, Reports and Minutes of meetings	Permanent
5.	Licenses Active	Permanent
6.	Expired Licenses	6 years after expiration
7.	Deeds and Titles	Permanent
8.	Leases Active	+ 6 years

9.	Policy Statements	Permanent
10.	Contracts Active	+ 4 years
11.	Insurance Documentation	+ 7 years

2.5 – Employee Applications and employment listings

No.	Employee Applications and Employment listings	Disposal (minimum period)
1.	Job announcements and advertisements	2 years
2.	Documentation on individuals not recruited	2 years
3.	Individuals who are hired recruited	+ 5 years
4.	Individual employee files and wage history active	+ 6 years

2.6 – Employee/ Personal files and payroll records

No.	Personal Files and Payroll Records	Disposal (maximum period)
1.	Employee files and documentation	Permanent (general in line with finance e.g. payroll)
2.	Salary or current rate of pay active	+ 6 years
3.	Payroll deductions active	+ 6 years
4.	Timesheets and expense claim active	3 years
5.	Employee manuals / handbook	Permanent
6.	Copy of payslips	+ 6 years
7.	End of year payslip, tax and pensions returns	Permanent

2.7 – Accounts and Financial Records

No.	Accounts and Financial Records	Disposal (maximum period)
1.	Billing Records	6 years
2.	Tax Returns	6 years
3.	Year Ends accounting records	Permanent
4.	General Ledger	6 years
5.	Account Ledger	6 years
6.	Auditor's report	Permanent
7.	Bank Statement	6 years
8.	Investment Details	Permanent

2.8 – Rate and land Records

No.	Rate and Land Records	Disposal (maximum period)
1.	Land Maps	Permanent
2.	Land Valuation	Permanent
3.	Ratepayer active	Permanent
4.	Previous ratepayer	Permanent
5.	Rate account	Permanent

2.9 - Health and Safety Records

No.	Health and Safety Records	Disposal (minimum period)
1.	Policies and Procedures	Minimum of year +5

2.	Risk Assessments and SSOW	Minimum of year +5
3.	Statutory Testing Documents (LOLER etc)	Minimum of year +5
4.	Accident Investigations, reports and investigations	Minimum of year +5
HR may request copy for Personal file – therefore the Personal File retention is followed		
5.	Asbestos exposure records	Minimum of 40 years
Disposal Responsibilities The Risk Manager will ensure that Health and Safety Documents are disposed of at the required intervals, if they are hard or soft copies and how the disposal has occurred.		

2.10 – Enforcement and Consent Case Records

No.	Enforcement and Consent Case Record	Disposal (maximum period)
1.	Land Maps	Permanent
2.	Land Valuation	Permanent

2.11 – Storage of documents

All data and records should be stored as securely as possible in order to avoid potential misuse or loss.

All data and records will be stored in the most convenient and appropriate location, having regard to the period of retention required and the frequency with which access will be made to the record.

Data and records which are active should be stored in the most appropriate place for their purpose. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

Any data file or record which contains personal data of any form can be considered as confidential in nature.

Paper copies of confidential documents will have key access.

Electronic copies of confidential documents - access rights granted via SharePoint.

2.12 – Disposal of documents

Records should be reviewed as soon as possible after the expiry of the retention period. It need not be a detailed or time-consuming exercise but there must be a considered appraisal of the contents of the record.

A record should not be destroyed without verification that:

- no work is outstanding in respect of that record and it is no longer required.
- the record does not relate to any current or pending complaint, investigation, dispute or litigation or

- the record is unaffected by any current or pending request made under the Freedom of Information Act or Data Protection Act.

A record must be made of all disposal decisions and destruction should be carried out in a manner that preserves the confidentiality of the record. Confidential paper records should be placed in confidential waste bins and electronic records will need to be either physically destroyed or erased to the current standard. Deletion of electronic files is not sufficient. All copies of a record, in whatever format, should be destroyed at the same time.

Example Deletion Form – Annex 1

Variation

Information needs are dynamic and therefore this policy is a “living" document which will be amended as the need arises.

Any review of retention periods should take account of relevant statutory and legal requirements and consideration of the overall operational value of records, including:

- on-going operational, accountability and audit needs.
- best practice in the applicable professional field.
- the probability of future use.
- the long-term historical or research value of the record.
- the costs of retention or destruction.
- the risks associated with retaining or destroying the record.

Other Records

Many records have no significant operational or evidential value and are not subject to retention under this policy but may be destroyed once they have served their primary purpose. These include:

- requests for forms and brochures.
- meeting rooms reservation requests.
- compliment slips and similar items which accompany documents.
- superseded distribution or mailing lists.
- drafts of documents.
- working papers which are the basis of the content of other documents.
- notices of meetings and other events.
- invitations and notices of acceptance or apologies.
- magazines, marketing materials, catalogues, directories, etc.

This is not an exhaustive list but merely indicates the types of record which have no significant operational or evidential value and may be destroyed once their effective use has ended.

2.2 – GDPR and Data Protection Policy

2.2.1 – Introduction to GDPR and Data Protection at the Boards

This policy covers records held and processed by the Boards. The Boards are responsible for their own records under the terms of the Act and it has submitted a notification as a Controller to the Information Commissioner.

The Boards are required to meet its legal obligations and requirements concerning confidentiality and information security standards.

The requirements within the Policy are primarily based upon the Data Protection incorporating the Data Protection Regulation 2016 and the General Data Protection Act 2018 which is the key piece of legislation covering security and confidentiality of Personal Confidential Information (PCI).

The policy is split into sections and details specific procedures for achievement of the policy standards.

2.2.2 - Scope

This policy applies to:

- All personal data processed by the Boards' regardless of its format.
- Any individual processing personal data held by the Boards'.

2.2.3 - Definitions

Data Protection Legislation means:

- The General Data Protection Regulation ("GDPR")
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations 2003 (as amended)
- Any other applicable law concerning the processing of personal data and privacy.

Data means information which:

- Is being processed wholly or partly by automated means.
- Is processed other than by automated means and forms part of a filing system i.e. structured set of data which are accessible by specific criteria.
- Is processed other than by automated means and is intended to form part of a filing system.

Personal data means

- Any information, which either directly or indirectly, relates to an identified or identifiable living individual. Identifiers include name, address, and date of birth, postcodes, unique identification numbers, location data, online identifiers (such as an IP address), pseudonymised data and information relating to a person's social or economic status.

Special Category Data means

personal data consisting of information as to:

- The racial or ethnic origin of the data subject.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- Physical or mental health or condition.
- Biometric and/or genetic data.
- Sex life or sexual orientation.

Criminal Convictions Data means

personal data consisting of information as to:

- The commission or alleged commission by him/her of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing in relation to information or data, means

any operation(s) performed on personal data or sets or personal data (whether automated or not) such as collection, use, storage, disclosure, dissemination and destruction.

Data subject means

an individual who is the subject of personal data.

Controller means

a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed. A controller may also act jointly with another organisation to process personal data.

Processor, in relation to personal data, means

any person or organisation (other than an employee of the controller) that processes data on behalf of the controller.

2.2.4 - The Six Data Protection Principles

The Boards shall adhere to the six principles of data protection, which are:

- Principle 1: Personal data shall be processed fairly and lawfully and in a transparent manner.
- Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes shall not be processed in a manner incompatible with that purpose.
- Principle 3: Personal data shall be adequate, relevant and limited to what is necessary for the purpose.
- Principle 4: Personal data shall be accurate and, where necessary kept up to date.

- Principle 5: Personal data shall be kept in a form that permits identification for no longer than necessary.
- Principle 6: Personal data shall be processed in a manner that ensures appropriate security.

In addition, the Boards shall ensure that they comply with the 'accountability principle' which requires that the Boards' has appropriate processes and records in place to demonstrate its compliance with the principles listed above.

2.2.5 - Record of Processing Activity

The Boards' shall maintain a written record of its data processing activities.

2.2.6 - Privacy Notices

To support open and transparent data processing the Boards shall ensure that privacy notices are made available to data subjects.

The Boards will adopt a layered approach to privacy notices i.e. Corporate / Directorate / Function (where necessary).

Privacy notices will be clear, concise, and in plain English.

A copy of any privacy notice shall be provided on request and free of charge.

2.2.7 - Data Protection Impact Assessment (DPIA)

The Boards aim to complete a DPIA at the early stages of any processing activity that involves high risk processing. Such activities include processing on a large scale; systematic monitoring; or processing special category data.

The DPIA shall be used to identify and remediate privacy risks.

Staff shall consult at an early stage to identify DPIA requirements.

The Chief Executive shall be consulted on all DPIAs.

2.2.8 - Data Security

The Boards shall ensure it has an information security management system in place that aims to reduce the risk of personal data breaches.

Security policies and procedures shall be made available to all staff.

The Boards' shall record and investigate all personal data breaches.

Where it is determined that a breach results in a risk to the rights and freedoms of an individual(s) will aim to report the breach to the Information Commissioner's Office within 72 hours of becoming aware.

Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the DPO shall inform the individual(s) without undue delay.

2.2.9 – Notification to Employees of GDPR/ Data Protection

Contracts shall include measures to ensure personal data is handled in accordance with data protection legislation.

Where contracts are not in place, or prior to legislation changes, an Employee Statement can be provided.

Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason.

The boards' shall ensure that before personal data is shared with a third party as part of a contract, appropriate security controls are in place.

2.2.10 - Information Sharing

The Boards' shall ensure that information is shared only when it is within the provisions of data protection legislation.

The Boards' shall ensure that when information is shared it is justified and necessary to meet a lawful basis for processing as set out at Appendix A to this policy.

The Boards' shall ensure that adequate security is in place to protect the data when it is shared with another organisation and that information sharing arrangements are documented.

The Boards' shall ensure that information sharing agreements exist between the Boards' and partnership agencies where required.

Guidance on information sharing in the context of systematic sharing and sharing in ad-hoc, one off circumstances.

2.2.11 - Individual Rights

The DPO shall ensure that adequate processes are in place to support individuals who wish to exercise their rights in respect of their personal data.

The DPO shall respond to any request to exercise individual rights within one calendar month.

Complaints regarding how the DPO processes personal data shall be referred to the relevant service area in the first instance and then to the Chief Executive if the matter cannot be resolved.

2.2.12 - CCTV

The CCTV access and security policy details the CCTV arrangements.

2.2.13 - International Transfers

Any systematic sharing of personal data outside of the UK shall be subject to a DPIA.

2.2.14 - Information Commissioner's Office (ICO)

The Boards shall comply fully with all requests from the Information Commissioner's Office to investigate and/or review their data processing activities.

The Boards shall have regard to advice and guidance produced by the Information Commissioner's Office as far as it relates to their data processing activities.

The Boards shall consider any code of practice published by the Information Commissioner's office and shall endeavour to align its own practices accordingly.

2.3 – Freedom of Information (FOI) Policy

2.3.1 – Introduction to FOI

The Freedom of Information Act 2000 came into force on 1 January 2000 and provides the public with a general right of access public information. This may, within the right circumstances include information held by the Boards.

The Boards have introduced a framework within this policy, under which FOI requests are received, processed, and completed in accordance with the Act.

The aim of this policy is to ensure the Boards meet their obligations under the Freedom of Information (FOI) Act 2000.

2.3.2 – FOI at the Boards

This policy applies to any recorded information which may be held by the Boards.

Employees should have an awareness and understanding of the FOI. However, if a request for information is received, no guarantee of information is to be provided, but the request to be passed through to SMT to determine if, and what (if anything) can be provided.

It is important to consider all aspects of the FOI in that it is not just the information provided, but the potential time taken to be reasonable and proportionate to provide such information.

2.3.3.- Principles of FOI at the Boards

The following principles shall apply:

- FOI covers any recorded information held by the Boards. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.
- FOI covers information that is held on behalf of the Boards even if it is not held on 4 Boards' premises.
- People shall have a right to know about the activities of the Boards, unless there is a good reason for them not to.

- An applicant (requester) shall not be required to provide a reason for requesting information. The Boards, however, shall justify refusing a request.
- The Boards shall treat all requests for information equally, except under some circumstances relating to vexatious requests and requests for personal data.
- The Boards shall treat all requestors equally regardless of who they are, for example journalists, local residents, public authority employees.

2.3.4 - Requests for Information under the Freedom of Information Act

Any written request for information shall be regarded as a request for recorded information under the Act unless:

- Information can be dealt with as a normal customer enquiry and therefore more sensibly, under the usual customer service procedures.
- It forms a request for personal data relating to the individual requesting the information. This shall be dealt with under data protection legislation, and consequently shall be processed in line with the Boards' Data Protection / GDPR Policy (Subject Access Requests.)
- A request shall only be accepted if in writing. E.g., online forms, letters or emails.
- Requests for information shall be met within 20 working days of receipt. A request under Environmental Information Regulations (EIR) can be extended to 40 days but only for complex or voluminous requests.
- Ambiguous requests shall be clarified with the requestor.
- A request for information shall not be refused because the recorded information is out of date, incomplete or inaccurate.
- The Boards shall not make any changes or deletions to records as a result of a request.

2.3.5 - Refusing a request

The Boards shall consider refusing a request for information under certain circumstances:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

The Boards shall consider refusing a request for information if the request meets an exemption under the Act. The Boards may also refuse to confirm or deny whether they hold information where the Act allows.

Legal advice may be sought before refusing a request to ensure the grounds for refusal are robust; justification will be required should the refusal be challenged.

A written refusal notice shall be issued to the requestor if the Boards either refuse to say whether they hold information at all or confirms that information is held but refuse to release it.

2.3.6 - Charges

The Boards shall make no initial charge upon the receipt of a FOI request.

If the FOI request is something which can be responded to without significant cost or staffing requirements, charges are unlikely to be applied. However, in some circumstances the Boards shall charge an appropriate fee for responding to requests for information.

The FOI itself and advice shall be sought from the Senior Management Team (SMT) if a fee is being considered and a detailed breakdown and explanation of charges will be supplied to the requester in all cases where a fee is requested.

2.3.7 - Complaints & Review Process

The Boards shall conduct a request review whenever the requestor expresses dissatisfaction with the outcome.

The review shall not be limited to the first decision but shall provide a new decision based on all available evidence that is relevant to the date of the request.

The review shall be done by someone who did not deal with the original request, and where possible by a more senior member of staff.

The Boards shall conduct a review within 20 working days; in exceptional circumstances this time limit shall be extended to 40 working days.

The Freedom of Information Act 2000 ("the Act") gives a general right of access to recorded information held by public authorities and sets out exemptions from that right and places several obligations on public authorities. The Boards are deemed to be non-departmental public bodies for the purposes of the Act. Further information about the Act can be obtained from The Information Commissioners Office (ICO) (link to the information commissioners office)

2.3.8 - What information is routinely available?

The Boards' information is grouped into seven classes.

1. *Who we are and what we do*
   Organisational information, structures, locations and contacts.
2. *What we spend and how we spend it*
   Financial information relating to projected and actual income and expenditure, procurement, contracts and audited accounts.
3. *What our priorities are and how we are doing*
   Strategies and plans, value for money indicators, audits, inspections and reviews.
4. *How we make decisions*
   Decision making processes and records of decisions.
5. *Our policies and procedures*
   Current written protocols, policies and procedures for delivering our services and responsibilities.

6. *List and registers*
   All statutory and non-statutory registers.
7. *The services we offer*
   Information about the services the Boards currently provide including leaflets, guidance and newsletters.

2.3.9 - How to access the information?

The information contained in each class may be accessed through a variety of means and in several formats where available. All information is available for inspection on request and by prior appointment, where appropriate copies, if appropriate, may be made available. A charge may be applied to the information supplied. Each case is considered individually. Information will be provided within 28 days if the request is reasonable.

Information can be accessed via:

- **The Witham and Humber Drainage Board website** [link to our website]
  Information is available on the web-site, and this information is non- chargeable.
- **E-mail**
  enquires@witham3idb.gov.uk
  Please use - 'Freedom of Information Request' in the subject line to allow identification
- **By post** – please address to:
  Jane Froggatt, Chief Executive Officer
  Witham House | Meadow Lane | North Hykeham | Lincoln | LN6 9TP
  Note - where hard copies of information are requested 1 copy will provided, and not multiple copies.
- **In person**
  Please contact the office via email or phone (01522 697 123) to arrange an appointment to attend Witham House.

2.3.10 - Charges and Exempt Information:

Charges may be imposed as standard for the provision of some of the information within this publication scheme.

Where a class contains information, which may levy a charge, this is made clear with a £ symbol shown below.

In adopting this scheme there has been an effort to be as open as possible but there are instances where, for legitimate reasons, certain information is not available. Where this is the case the reasons behind the decision to exclude certain information is clearly stated.

Justification for excluding information is made in consideration of the general exemptions contained in the Act, the Environmental Information Regulations, the Data Protection Act or where it may be of a confidential or commercially sensitive nature.

2.3.11 - The Information Available:

1. *Who we are and what we do*
   Constitution of the Board, including their structure & membership Staffing Structure
   Geographical area covered
   Outline of responsibilities
   Location of offices and contact details
2. *What we spend and how we spend it (£)*

   Annual accounts
   Audit of accounts
   Revenue and capital spending plans Procurement Regulations

   Funding: details of drainage rates, special levies, grants and other financial contributions
   Staff and Board members allowances and expenses
   Contracts awarded and their value
3. *What our priorities are and how we are doing (£)*

   Aims, objectives and plans
   Performance against aims and plans
   Programme of works
4. *How we make decisions*
   Board meeting and sub-committee minutes. Public consultations
   Reports of advisory groups
   Environmental Impact Assessments Assessment of flooding risks
   Other publicly available reports
5. *Our policies and procedures*
   Policies and procedures for the conduct of the Boards' business, the provision of services, employment matters
   Whistle blowing policy
   Anti-fraud & corruption policy
   Data protection policy, including GDPR, FOI and Documents Retention.
   Customer complaints procedure
   Charging regimes and policies [e.g. Enforcement and Consent applications]
6. *List and registers (£)*
   Register of Drainage Infrastructure
   Nuisance Register
   Complaints Register
   Rate Book
   Electoral Register (for the purposes of an Election of IDB Members)

   Register of Members' Interests

Members' Attendance Register
Freedom of Information Act disclosure log

7. *The services we offer (£)*
   Regulatory role
   Byelaws
   Information for landowners, developments and operations Notices, leaflets and guidance

Media releases - Details of the services for which the Board is entitled to recover a fee together with those fees

3.0 – Document retention and Document Policy Statement

The Boards recognise the importance of processing, holding and archiving our documents.

The Boards will comply with the policy by:

- Making this policy easily accessible.
- Following the policies consistently within for transparency and fairness to employees.
- Keep the policies updated where any changes in legislation or ADA white book.
- Ensure that employees understand the policy and how this may apply to them.
- Following this policy at all times.

4.0 - Glossary / Definitions

Word/ term	**Definition**
GDPR	General Data Protection Regulations
FOI	Freedom of Information
EIR	Environmental Information Regulations
ICO	Information Commissioners Office

5.0 – Legislation

- Freedom of Information Act 2000 (link to FOI Legislation)
- The Equalities Act 2010
- Data Protection Regulation 2016
- General Data Protection Act 2018
- The Rehabilitation of Offenders Act, 1974
- GDPR and Data Protection legislation.
- ADA Lincolnshire Branch White Book 2024 [as the current version]

6.0 - Main policy Roles and Responsibilities

6.1 Arrangements for roles and reporting lines

The arrangements and organisational responsibilities for implementing the policy are detailed in this section.

6.1.1 – Board Members

- Approve and support the Senior management Team with this policy.
- Support the Chief executive Officer and SMT in following the Policy.

6.1.2 – Chief Executive Officer (CEO) and Senior Management Team (SMT)

- Lead by example.
- Offer guidance and support to any team members who may require it.
- Pay the annual statutory data protection fee to the Information Commissioner's Office. The Boards'' data protection registration number is (insert the requirement for each Board)
- Review the appropriate policies and processes.
- It has access to specialist staff with specific responsibility for providing support and guidance to the Boards'.
- Staff processing personal data understand that they are responsible for complying with the data protection principles and are appropriately trained.

6.1.3 - Specifically Associate Director of HR

- Lead the Policy as necessary and facilitate the onboarding process.
- Provide support/guidance to line managers during onboarding.
- Monitor composition of workforce to identify areas that may need positive action measures to promote Equality, Diversity and Inclusion.
- Be responsible with the appointing team for selecting the right candidate for the role.
- Ensure all persons on the interview panel are trained commensurate with their role.

- Ensure there are no conflicts of interest on the interview panel.
- Ensure no start date is provided before all pre-employment checks are complete.
- Advertise the role(s) on appropriate platforms and provide advice for best practice.
- Keep required and relevant onboarding records for the process and for onboarding. Records not required, will be securely destroyed.
- Ensure that any 'reasonable adjustments' are in place prior to new starter with reviews in place to ensure they remain suitable and sufficient.

6.1.4 – Data Protection Officer (DPO)

- The organisation will have in place a DPO responsible for supporting the Chief Executive in meeting the obligations under data protection legislation.

The role, which is a statutory requirement, will:

- Monitor ongoing compliance.
- Provide advice and guidance on all data protection matters.
- Act as a point of contact for all data subjects.
- Act as the single point of contact for the Information Commissioner's Office and any other bodies engaged in the application of data protection legislation.

6.1.5 – Data Protection Roles and Responsibilities

In addition to the DPO the following roles are established:

- The owner of information risk management at director level and is responsible for leading and fostering a culture that values, protects and uses information in a manner which benefits the boards', employees and the individuals and community who use the Boards' services.
- responsible for the assurance of information, identification, management and implementation of information risk.
- responsible for providing governance support, guidance, and training to the Boards' ensuring that staff are aware of their data protection responsibilities and obligations.
- ensure that specific information assets are handled and managed appropriately, key decision makers across information they own.
- All line managers are responsible for ensuring that the requirements of this policy are integrated into service procedures and that staff comply with all relevant policies in their area of responsibility.
- All Staff are responsible for ensuring they process information in line with this policy. This includes complying with related policy requirements and undertaking training.

6.1.6 – Risk Manager

- Support SMT with the review and update of this policy.

6.1.7 – Line Managers / Supervisors / Foremen

- Support the CEO & SMT to cascade the policy.

- Follow requirements within this policy.
- Obtain advice, guidance and information from Associate Director for HR.
- Work with the Associate Director for HR for selecting the right candidate for the role.
- Provide support, mentoring and assistance during onboarding process.
- Provide a 'buddy' or mentor for the new starter to ensure that ongoing learning and support is provided during the early stages of employment.

6.1.8 – Staff members

- Must follow the Employees Code of Conduct and follow required standards and behaviours.
- Raise any queries with their line manager.
- Work with colleagues and line manager to learn as much as possible.
- Continue with 2-way communication to ensure rapports are built and relationships are fostered within the working environment.

7.0 - Document review:

Version	Date	Reviewed by	Changes	Approved by/ date
1.00	2020	Ass Director for HR	• Board approved Document Retention Policy	JSC July 2020
5.00	2020	Ass Director for HR	• Board approved GDPR Policy	JSC July 2020
2.00	2020	Ass Director for HR	• Board approved FOI Policy	JSC July 2020
1.00	2024	Risk Manager and Ass Director for HR	• Updated lay out, general review • Incorporating v1 document retention policy, v5 GDPR policy and v2 FOI policy. • Renaming as Document Retention and Privacy Policy	JSC December 2024

This policy is due for review at 5 yearly intervals, unless a review is required before e.g. change to management, process or anything which may affect the contents of this policy.

8.0 - Supporting documents

ANNEX 1 – Example Deletion record

ANNEX 1 – Example Deletion Record

Deletion Log

This document can be held and documents how and what is being deleted.

Document(s)	Date left Cope Due to deletion	How deleted (manual – shred; e-document – delete etc.)	Deleted by whom and date