Doncaster East Internal Drainage Board

DATA PROTECTION
PRIVACY AND BREACH POLICY

CONTENTS

1. Policy Statement

1:1 During the course of our activities we will collect, store, process and share information about individuals and we recognise the need to treat it in an appropriate and lawful manner. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

1:2 The Board is obliged under Data Protection legislation to have policies and procedures in place to ensure the security of all personal data. This policy sets our rules on data protection, purposes for processing personal data, categories of the personal and sensitive data held, retention periods, privacy notices, data subject rights and subject access requests. As well as the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents, to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

1:3 The Board is a data controller and data processor as defined by the General Data Protection Regulations 2016 (GDPR) and Data Protection Act 2018. Our full details are:

Doncaster East internal
Drainage Board
Wellington House
Manby Park
Manby, Louth
Lincolnshire
LN11 8UU

Tel: 01507 328095

enquiries@deidb.co.uk

1:4 The Board has appointed a Data Protection Officer who can be contacted on

governance@deidb.co.uk

1:5 Full contact details can be found on the data protection page of our websites:

https://www.deidb.co.uk/

1:6 The Board must be able to demonstrate compliance with the legislation and this policy sets out its procedures for compliance.

2. Data Protection

2:1 The Board process data to allow us to perform our statutory function under the Land Drainage Act 1991 and to enforce our Byelaws. This includes issuing Drainage Rates and Special Levies, Notices of Entry, Byelaw Consents and processing enquiries.

2:2 Personal Data is defined by data protection legislation as any information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2:3 The Board process a number of types of information which includes but is not limited to: name, address, telephone number, date of birth, national insurance number and bank details.

2:4 For their employees, volunteers and members, the Board may also process Special Category Personal Data such as biometrics, health, political and union membership.

2:5 Article 5 of the GDPR sets out six principles covering the Board's responsibilities and requires that data be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) 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);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals; and

(f) 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.

3. Processing

3:1 The Regulations state that in order to process personal data the Board must rely on one or more of six lawful bases. We will notify individuals of this basis when the data is collected in the form of a Privacy Notice. Should there be any change in our legal basis for processing personal data (provided the purpose is compatible with the original purpose) the individuals affected will be notified in writing of the new legal basis on which the Board is relying.

3:2 Legal Bases:

(a) Consent

Clear consent has been given for the processing of personal data for a specific purpose.

(b) Contract

The processing of personal data is necessary for a contract between the Board and individual.

(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 its official functions.

(f) Legitimate interests

The processing is necessary for the Board legitimate interests.

3:3 Personal Data may be obtained directly from individuals or from third parties including, but not limited to, solicitors, land agents, land registry and local councils.

4. Special Category Data

4:1 The Board process a limited amount of Special Category Data for their Employees, Volunteers and Board Members. In order to process special category data the Board must have an second condition in addition to the lawful basis for processing as outlined in section 3 above.

4:2 These conditions as detailed in Article 9(2) of GDPR are:

(a) The data subject has given explicit consent to the processing;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) Processing relates to personal data which are manifestly made public by the data subject;

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 of the legislation;

(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4:3 The Board processes most of its Special Category Data through reliance on Article 9(2)(b) Employment listed above. The condition used to process special category data will be listed in our Privacy Notice.

4:4 Access to Special Category Data is limited to reduce the risk of any data protection breach. All files are kept locked with access to them restricted and computer programmes are password protected.

5. Data Subject Rights

5:1 The law gives individuals a number of rights to control what personal information is collected by us and how it is used. The Board will respond to any requests within 28 days unless the request is complex. For complex requests Board will respond within 84 days, however, we will inform you of the date you will receive the information if this extension is applied.

5:2 Your rights are listed below:

(a) Right to be informed

When personal information is collected about you the Board will issue you with a Privacy Notice which explains what information we hold, why we hold it, how long it is held and which of your rights (listed below) apply to that data. Copies of the Board's Privacy Notices can also be found on our website.

(b) Right of access

You have the right to ask for information the Board holds about you.

Requests for information (Subject Access Requests) should be made in writing, if you are unable to make your request in writing please contact the office to discuss your needs. A copy of the Board's Subject Access Request Form is available from the office or can be found on the Data Protection page of the Board's website. This applies to personal information that is in both paper and electronic records.

We can't let you see any parts of your record which contain:

- Confidential information about other people; or
- Data a professional thinks will cause serious harm to your or someone else's physical or mental wellbeing; or
- If we think that giving you the information may stop us from preventing or detecting a crime.

(c) Right to rectification

Individuals have the right to ask for the information held by the Board to be updated if it is incorrect or incomplete. Whilst the Board makes efforts to ensure the data we hold is accurate we recognise that amendments may need to be made.

The Board may need to ask for clarification or confirmation of identity to action some requests. On occasion, we may refuse to amend the information we hold, if this occurs we will inform you of the reasons for this decision.

(d) Right to erasure

In some circumstances individuals have the right to request their information be erased. The Board may ask for confirmation of identity before actioning a request for erasure.

This right only applies if:

- The personal data is no longer necessary for the purpose which we originally collected or processed it for;
- We relied on consent as our lawful basis for holding the data, and you withdraw your consent;
- We are relying on legitimate interests as our basis for processing, you object to the processing of your data, and there is no overriding legitimate interest to continue this processing;

- We are processing the personal data for direct marketing purposes and you object to that processing;
- We have processed the personal data unlawfully; or
- We have to do it to comply with a legal obligation.

The legal basis used for processing personal information is detailed in the relevant privacy notice. If a request for erasure is refused a notice will be issued detailing our reasons for this decision.

(e) Right to restrict processing

In some circumstances individuals have the right to restrict the processing of their personal data. This right usually applies when a request for rectification has been made.

Examples of instances when individuals can restrict the processing of their personal data are as follows:

- The individual contests the accuracy of their personal data and the Board is verifying the accuracy of the data;
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- The Board no longer needs the personal data but the data subject needs us to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to the Board processing their data, and we are considering whether our legitimate grounds override those of the individual.

(f) Right to data portability

This right gives individuals the ability to receive their personal data in a machine-readable format or request that it be passed to another data controller.

Only a very small amount of the data held by the Board may be subject to this right, which only applies if the Controller is carrying out the processing by automated means and to data processed with Consent or Contract as our legal basis for processing.

(g) Right to object

This right allows individuals to object to the processing of their data for direct marketing.

Individuals can also object to processing of data for other purposes:

- A task carried out in the public interest;
- The exercise of official authority; or
- Legitimate interests (or those of a third party).

Provided that they have a compelling reason to do so.

If this right applies to the data collected it will be stated on the privacy notice issued at the point of collection.

(h) Rights relating to Automated Decision Making and Profiling

Whilst not currently undertaken by the Board, legislation also gives individuals rights in relation to automated decisions and profiling.

Whilst not an absolute right, individuals can also object if the processing is for:

- A task carried out in the public interest;
- The exercise of official authority vested in the Board; or
- Legitimate interests (or those of a third party).

Any objections should include specific reasons why the objection is being made.

5:3 The Board has produced a Guidance Note which details explains in detail the rights of Individuals under current legislation. This is available on the Data Protection page of the Board's website.

6. Retention

6:1 The Board will keep personal data only as long as it is necessary to do so. Some data must be retained for the Board's compliance with legislation. The Board has adopted a Document Retention Policy which outlines how long data will be held. When personal data is collected a Privacy Notice will be issued giving details of the retention period for that data.

6:2 A copy of the Board's Document Retention Policy can be found on the Data Protection page of the Board's Website.

7. Data Protection Breaches

7:1 This section relates to all personal and special category data held by the Board regardless of format. This section of the policy applies to all Board Members, staff and students including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Board.

(a) Definitions and Types of Breach

7:2 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

7:3 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Board's information assets and/or reputation.

7:4 An incident includes but is not restricted to, the following:

(a) Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, mobile / tablet device, or paper record);

(b) Equipment theft or failure;

(c) System failure;

(d) Unauthorised use of, access to or modification of data or information systems;

(e) Attempts (failed or successful) to gain unauthorised access to information or IT system(s);

(f) Unauthorised disclosure of sensitive / confidential data;

(g) Website defacement (including social media accounts);

(h) hacking attack;

(i) Unforseen circumstances such as a fire or flood;

(j) Human error;

(k) 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

(b) Reporting an Incident

7:5 Any individual who accesses, uses or manages the Board's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer, Chief Executive or Corporate Services Manager and the IT Specialist.

7:6 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable, but no longer than 24 hours following discovery.

7:7 The report should include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. A Data Breach Reporting Form should be completed as part of the reporting process.

7:8 All staff should be aware that any breach of Data Protection legislation may result in the Board's Disciplinary Procedures being instigated.

(c) Containment and Recovery

7:9 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and an investigating officer will be appointed who will take the lead investigating the breach.

7:10 The Investigating Officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. They will establish who may need to be notified as part of the initial containment, will inform the police where appropriate and, in liaison with the relevant officer(s), determine the suitable course of action to be taken to ensure a resolution to the incident.

7:11 This process will be monitored throughout by the Chief Executive.

(d) Investigation and Risk Assessment

7:12 An investigation will be undertaken immediately and wherever possible, within 24 hours of the breach being discovered/reported. The Investigating Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7:13 The investigation will take into account the following:

(a) The type of data involved;

(b) Its sensitivity;

(c) The protections that are in place (e.g. encryptions);

(d) What has happened to the data (e.g. has it been lost or stolen);

(e) Whether the data could be put to any illegal or inappropriate use;

(f) Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);

(g) Whether there are wider consequences to the breach.

(e) Notification

7:14 The Investigating Officer and/or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7:15 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

(a) Would the breach be likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;

(b) Would notification assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

(c) Would notification help prevent the unauthorised or unlawful use of personal data;

(d) Any legal/contractual notification requirements;

(e) The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7:16 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Board for further information or to ask questions on what has occurred.

7:17 The Investigating Officer and/or the DPO must consider notifying third parties such as the police, insurers and banks or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7:18 A record will be kept on the Board's Breach Log of any personal data breach, regardless of whether notification was required.

(f) Evaluation and Response

7:19 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies

and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

7:20 The review will consider:

(a) Where and how personal data is held and where and how it is stored;

(b) Where the biggest risks lie including identifying potential weak points within existing security measures;

(c) Whether methods of transmission are secure; sharing minimum amount of data necessary;

(d) Staff awareness;

(e) Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security;

(f) The outcome of the review will be reported to the Chief Executive.

7:21 If deemed necessary, a report recommending any changes to systems, policies and procedures will be prepared for consideration by the Board.

(g) Review

7:22 The Board's data breach procedure will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

8. Complaints Procedure

8:1 Any concerns or questions about how personal information is handled should be addressed in the first instance to our Data Protection Officer at:

Email - governance@deidb.co.uk

Tel - 01507 328095.

8:2 If you would like to raise a formal complaint this should be made using the process outlined in our complaints procedure. If necessary, the Board will report any breach to the ICO as outlined in section 7.

8:3 If you are dissatisfied with the Board's response or for independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO) at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113.

Alternatively, visit ico.org.uk or email casework@ico.org.uk.

9. Data Sharing

9:1 The Board will share personal data with employees and members of the Lindsey Marsh Drainage Board. This data will be subject to the same security measures by both Boards and in line with the data sharing agreement signed by the Boards. In some instances data may also be shared with contractors who act as data processors, should this occur an appropriate data protection compliant agreement will be in place.

9:2 Personal data may also be shared with third parties where required to do so by law (for example with HMRC, Police etc).

9:3 The Board uses off site data storage to back up its data, this data is held within the European Economic Area (EEA) and is subject to Data Protection Legislation. The Board regularly review the security of this data.

9:4 The Board does not routinely transfer data outside the EEA and any such transfers would only be made at the request of the individual.

10. Security

10:1 The Board will ensure that within the best of their abilities they hold records about you (on paper and electronically) in a secure way, and will only make them available to those who have a right to see them. Examples of our security measures include:

(a) Encryption - information is hidden so that it cannot be read without special knowledge (such as a password).

(b) Pseudonymisation - Use of a different name or random number so we can hide parts of your personal information from view.

(c) Access Restriction - Controlling access to systems and networks to stop people who are not allowed to view personal information from getting access to it.

(d) Training - Staff training to make them aware of how to handle information and how and when to report when something goes wrong.

(e) System Testing - Regular testing of our technology and ways of working including keeping up to date on the latest security updates.

(f) Audits - Regular audits of our policies, processes and systems to ensure compliance.