Upper Medway Internal Drainage Board
General Privacy Notice (Website)

Your personal data – what is it?

"Personal data" means information relating to an identified or identifiable living individual. An individual may be identified directly, for example by name, or indirectly by combining information such as a personnel number with another record. Personal data includes names, contact details, photographs and video recordings where individuals are identifiable. We process personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025. The Privacy and Electronic Communications Regulations 2003 (PECR), as amended, also apply where relevant to electronic marketing and website storage and access technologies.

Who are we?

Upper Medway Internal Drainage Board (the Board) is the controller responsible for the personal data it processes for its drainage, water-level management and related administrative functions. This general notice explains our use of personal data concerning people who contact or deal with the Board, including ratepayers, landowners, applicants, suppliers and members of the public. Activity-specific information, including employment and CCTV privacy information, supplements this notice where relevant. Our contact details and the route to our Data Protection Officer are set out below.

Organisations with which we may share personal data, where necessary:

- Local authorities
- Contractors

An organisation receiving personal data is not automatically a separate controller. Contractors processing data solely on our behalf act as processors under our documented instructions and a binding agreement meeting Article 28 UK GDPR. An organisation deciding its own purposes and means is an independent controller. Where we jointly determine purposes and means with another controller, we will put an Article 26 arrangement in place, make its essence available to you and explain the contact arrangements. You may exercise your rights against any joint controller. The Board remains responsible for its own processing and for meeting its obligations when appointing processors.

We provide relevant privacy information when we collect data from you. Where we obtain it from another source, we provide information about the categories and source, including whether it is publicly available, within the applicable legal timescale: normally within one month, or earlier at our first communication with you or first disclosure to another recipient. Any statutory exception must be assessed individually; simply publishing this notice is not a substitute for actively providing privacy information where required.

The organisation will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;

- Information relevant to your dealings with the Board, including land or property interests, drainage-rate accounts, applications, correspondence, complaints and financial transactions. We collect only the information necessary for the particular purpose; employment-related information is addressed in the relevant employment privacy information.
- Where necessary for a specified purpose, we may process special category data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify a person, health information, or information about sex life or sexual orientation. These are not routine requirements for dealing with the Board. Criminal conviction, allegation and offence data are a separate category governed by Article 10 UK GDPR, not special category data under Article 9.

- How we use sensitive personal data

We may process sensitive personal data including, as appropriate:

- information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
- your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

- information necessary to meet a specific legal requirement; an obligation to a third party does not by itself authorise processing of special category data.
- Special category data requires both an Article 6 lawful basis and a separate Article 9 condition. Where required, we must also meet a condition in Schedule 1 of the Data Protection Act 2018 and maintain an appropriate policy document covering safeguards, retention and erasure. We identify the applicable condition for the particular processing and explain it in the relevant privacy information.

- We may process special categories of personal data in the following circumstances:

- With your explicit consent under Article 9(2)(a), where consent is freely given, specific, informed and capable of withdrawal. Written consent is not the only legally valid form of explicit consent.
- Where necessary for obligations or rights under employment, social security or social protection law: Article 9(2)(b) and Schedule 1, Part 1, paragraph 1 of the Data Protection Act 2018, with the required safeguards.
- Where necessary for reasons of substantial public interest under Article 9(2)(g), but only where a specific applicable Schedule 1 condition and its safeguards are met; a general public interest is not sufficient.
- Where necessary for legal claims under Article 9(2)(f); to protect vital interests where the individual is physically or legally incapable of consenting under Article 9(2)(c); or where the individual has manifestly made the information public under Article 9(2)(e). These conditions do not authorise unrelated or excessive use. Criminal offence data requires an Article 6 basis and either specific official authority or authorisation under domestic law, including an applicable Schedule 1 condition and safeguards. Public-body status alone does not supply that authority.

Do we need your consent to process your sensitive personal data?

Where we rely on explicit consent, we will explain the information, specific purpose and how to withdraw consent before seeking it. Consent is not the default basis for employment processing or the exercise of our statutory functions. Where another lawful basis and Article 9 condition apply, we will explain them rather than request consent that is not genuinely optional.

The organisation will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction or damage, and disposed of securely when no longer required.

We use your personal data for some or all of the following purposes:

- To administer drainage and water-level management work, communicate with affected landowners and occupiers, and deal with drainage enquiries and applications;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and protect public funds where supported by an identified lawful basis. Any processing by the Board as a competent authority for criminal law-enforcement purposes requires a separate assessment under Part 3 of the Data Protection Act 2018 and appropriate privacy information; this notice does not itself authorise such processing.
- To administer drainage rates, land and property records and Board governance, and exercise applicable statutory powers and duties;
- To handle complaints and undertake safeguarding or due diligence where necessary and supported by an identified lawful basis and any additional sensitive-data condition;
- To communicate about the Board's statutory work; optional promotional communications are treated separately from essential operational or statutory communications.
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff and other role holders;
- To send you communications which you have requested and that may be of interest to you.
- To process relevant financial transactions including grants and payments for goods and services supplied to the organisation.
- To allow the statistical analysis of data so we can plan the provision of services.

Where CCTV or vehicle cameras are used, processing must be necessary and proportionate to specified security or safety purposes, such as protecting people, premises and operational assets and providing evidence of incidents. Relevant signage and CCTV privacy information explain the controller, purposes, contact route and retention arrangements. Consent is not the default basis; each system requires a documented lawful basis and assessment under the Board's CCTV Policy.

What is the legal basis for processing your personal data?

Public task — Article 6(1)(e) UK GDPR: we use personal data where necessary to exercise the Board's official authority or perform its public tasks, including drainage and water-level management, drainage-rate administration and related governance under the Land Drainage Act 1991, as amended. A statutory power is not automatically a legal obligation to process data. Legal obligation — Article 6(1)(c): we use data where necessary to comply with a specific duty, for example applicable accounting, audit, tax or information-access requirements. We identify the relevant duty for the particular activity. We do not rely on legitimate interests or recognised legitimate interests to perform our public tasks.

Contract — Article 6(1)(b): we use personal data where necessary to enter into or perform a contract with you as an individual, including steps you request before entering that contract. This basis does not apply merely because work is delivered by a contractor, or where a contract is with a company rather than you personally; the appropriate public task or other lawful basis must be identified instead.

Consent — Article 6(1)(a): where participation is genuinely optional, for example optional communications for which consent is required, we obtain valid consent and explain how to withdraw it. Withdrawal does not affect earlier lawful processing. Where PECR requires consent for electronic marketing or website technologies, we obtain it unless a specific statutory exception applies and its conditions are met. At the point of collection we explain whether providing information is a statutory or contractual requirement, whether you must provide it and the specific consequences of not doing so. Missing necessary information may prevent us from dealing with an application, enquiry or contract, but withholding optional consent does not remove your statutory rights.

Sharing your personal data

We share only information necessary for a specified lawful purpose. Recipients must protect personal data, but their responsibilities depend on whether they act as processors, independent controllers or joint controllers, as explained above. We remain responsible for the Board's processing. Sharing may include the following categories where relevant:

- Local authorities and other public bodies where necessary for statutory functions or a specific legal disclosure requirement;
- Agents, suppliers and contractors supporting Board operations, including clearance works and services processing information on our behalf. Their role and access must be limited to the work they undertake.

How long do we keep your personal data?

We retain personal data only for as long as necessary for its purpose, in accordance with the Board's Data Retention and Disposal Policy and retention schedule. The period is determined by the record category, relevant statutory minimums, operational need, accountability and audit requirements, and the need to establish, exercise or defend legal claims. Claim limitation periods are not universal retention rules: the applicable period and its starting point depend on the circumstances. Records subject to an investigation, litigation or other justified legal hold are

preserved until the hold ends. Permanent retention is limited to records with a justified legal or public-interest archiving purpose and appropriate safeguards. When retention is no longer justified, data is securely destroyed or anonymised. You can request the period and retention trigger applicable to your information using the contact details below.

Your rights and your personal data

You have the rights described below. Some rights depend on our lawful basis and the circumstances, and statutory exemptions may apply. You can make a request verbally or in writing without using a special form. If we cannot comply, we will explain why, subject to lawful restrictions, and tell you about complaining to the Board, complaining to the ICO and seeking a judicial remedy.
We ask for additional identity information only where we have reasonable doubts about your identity, and only to the extent necessary and proportionate. We respond without undue delay and normally within one calendar month of the relevant starting point under the law. Where necessary because of the complexity or number of requests, we may extend by up to two further months and explain the extension within the initial month. For access requests, we may pause the period where clarification is reasonably required to identify the information or processing requested; we explain what is needed and resume the period when sufficient clarification is received.

The right to access personal data we hold on you

You can ask whether we process your personal data and obtain a copy, together with information about purposes, categories, recipients, retention, sources, rights and any relevant automated decision-making. We carry out reasonable and proportionate searches and protect other people's rights when responding. The response times and identity-check arrangements above apply.
Exercising your rights is normally free. We may charge a reasonable fee for further copies of information already supplied. Where a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse to act, as permitted by law, explaining and justifying the decision. A further request is not chargeable simply because you have requested information before.

The right to correct and update the personal data we hold on you

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

The right to have your personal data erased

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.

Erasure is not an absolute right. We will explain whether we have erased the data or why an exception applies, for example where processing remains necessary for a legal obligation, a public task or legal claims.

The right to object to processing of your personal data

You may object, on grounds relating to your particular situation, to processing based on our public tasks or official authority. We must stop unless we demonstrate compelling legitimate grounds overriding your interests, rights and freedoms, or the processing is necessary for legal claims. You have an absolute right to object to direct marketing,

including related profiling, and we will stop using your information for that purpose. Contact us using the details below.

The right to restrict processing

You may request restriction where you contest accuracy while we verify it; where processing is unlawful but you oppose erasure; where we no longer need the data but you need it for legal claims; or while we assess an objection. Where restriction applies, we may store the data but other processing is limited to the circumstances permitted by law. We will tell you before lifting a restriction.

The right to data portability

Portability applies to personal data you have provided where processing is automated and based on consent or a contract with you. You may receive it in a structured, commonly used, machine-readable format and ask us to transmit it directly to another controller where technically feasible, without adversely affecting others' rights. It does not apply to processing based on public task or legal obligation. The general response times above apply.

The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

Where we rely on consent, you may withdraw it at any time by contacting us using the details below or using the withdrawal option offered when consent was obtained. Withdrawal must be as easy as giving consent. It does not affect processing that was lawful before withdrawal, or separate processing supported by another lawful basis.

The right to complain about the use of your personal data

You can complain directly to the Board using the contact details below; no special wording or form is required. We will acknowledge receipt within 30 days, make appropriate enquiries without undue delay, keep you informed of progress and tell you the outcome without undue delay. If you remain dissatisfied, you can complain to the Information Commissioner's Office (ICO), the UK data protection regulator, using its complaints service or by calling 0303 123 1113. You may also seek a judicial remedy.

Automated decision-making

If we propose to make a decision with legal or similarly significant effects on you solely by automated processing, including profiling, we must first meet Articles 22A–22D UK GDPR and provide the required information about the processing, logic, significance and envisaged consequences. Applicable safeguards include information about the decision, the ability to make representations, obtain human intervention and contest the decision. Additional restrictions apply where special category data is involved. Contact the Board to ask about the decision-making arrangements relevant to your information.

Transfer of Data Abroad

A restricted transfer of personal data to a separate organisation outside the United Kingdom must meet UK GDPR transfer requirements. Where such a transfer is necessary, we rely on applicable UK adequacy regulations, appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum to EU standard contractual clauses, or a specific statutory exception where its conditions are met. Where safeguards require it, we carry out and document the data protection test (transfer risk assessment). We provide relevant information about the destination and applicable mechanism in the activity-specific privacy information, and you may request details or a copy of the safeguards using the contact details below, subject to necessary redactions. Availability of a public website overseas is not itself a substitute for assessing supplier hosting, overseas access and other data transfers.

Further processing

Before using personal data for a further purpose, we assess the applicable lawful basis and any compatibility requirements and provide the required information about that purpose and processing conditions before the further processing begins, unless a specific statutory exception applies. Where consent is required, we obtain it first. A new purpose is not automatically lawful simply because this notice has been updated.

Changes to this notice

We keep this Privacy Notice under regular review and publish updates on the Board's website. This notice was last updated in November 2026. Where changes affect how we use your information, we provide further privacy information as required by law.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Upper Medway IDB Data Protection Lead / Clerk: Email: enquiries@medwayidb.co.uk
You may contact our Data Protection Officer, Richard Newell (GDPR-Info.com), through the Clerk using the email above. Please mark correspondence "For the Data Protection Officer"; the Clerk's operational data protection role is distinct from the DPO's independent advisory and monitoring role.

November 2022 Amendments

- Removed LMIDB references
- Minor formatting alteration

November 2024 Amendments

- Minor date changes to reflect website

November 2026 Amendments

- Updated the legal framework to UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, with relevant PECR requirements.
- Clarified the Board's statutory drainage role and distinguished public task, specific legal obligations, contract and consent as lawful bases.
- Corrected special category and criminal offence data requirements, including additional conditions and safeguards.
- Clarified controller, joint-controller and processor responsibilities and the provision of privacy information for indirectly obtained data.
- Replaced generic retention and overseas-transfer wording with purpose-based retention criteria and UK transfer requirements.
- Corrected individual rights, access-request timescales and fees; separated objection and restriction and added current automated-decision safeguards.
- Added the statutory right to complain to the Board, acknowledgement within 30 days and investigation/outcome requirements; clarified the independent DPO contact route.