



February 2026
Version 2.0

EMPLOYEE PRIVACY NOTICE

This notice applies to current and former employees, candidates for new positions, contractors, and volunteers. This notice does not form part of any contract of employment or other contract to provide services. This notice can be updated at any time and we will notify if this occurs.

It is important that you read this notice, together with any other privacy notice that is provided on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using such information.

Contact details

	Address	Phone	Email
Data Controller Mater Misericordiae University Hospital ("MMUH", "we", the "Hospital" or the "Mater Hospital")	Eccles St Dublin 7 D07 R2WY	+353 (01) 803 2000	ceooffice@mater.ie
MMUH Human Resources Department ("HR")	Station Mews, Lindsay Grove, Dublin 9 D09 W8W8	+353 (01) 803 2686	humanresources@mater.ie
MMUH Data Protection Office	Eccles St Dublin 7 D07 R2WY	+353 (01) 803 4311	dataprotection@mater.ie

Data protection legislation

All personal data described in this notice will be processed in accordance with all applicable data protection laws and principles, including the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and the Data Protection Acts 1988 – 2018 (as amended).

For more information on Data Protection, we recommend the Data Protection Commission website <https://www.dataprotection.ie/en/individuals>.

What information we process

We collect, store and use (“**process**”) the following personal data about you:

- **Identity data:** first name, last name, other given, current, or former names, marital status, title, date of birth, gender, username, or employee ID number.
- **Contact details:** addresses, telephone numbers, personal email address, and next of kin or emergency contact details.
- **Monitoring data:** photographs and video (i.e. staff ID card, CCTV footage) and information obtained through electronic means such as swipe card records and your use of information and communication systems (See [PPS-ORG-019 - CCTV Policy](#)).
- **Recruitment data:** copy passport or other national identification document, birth certificate, right to work information (e.g. visa and work permit details), copies of proof of address documents (e.g. bank statements or bills), employment history (information included in your job application, employment references), notes in relation to the application, interview and contract formation process.
- **Financial and tax data:** Personal Public Service Number (“PPSN”), tax status information, pension and benefits details, bank account details, salary information (e.g. start and leave dates, changes to employment contract or working patterns), time spent working (e.g. timesheets or clocking in and out), expenses, allowances, overtime or other payments claimed, leave (e.g. sick leave, holidays, or special leave) and maternity, paternity, shared parental and adoption leave and pay, and trade union dues), compensation history and payroll records, and information supplied to and from the Revenue Commissioners.
- **Employment data:** role, start and leave dates, location of employment, secondary employment, education history (e.g. qualifications), security clearance details (e.g. basic checks and higher security clearance), performance records (e.g. reviews, disciplinary records, complaints or disciplinary actions), work history, working hours, training history, and development needs, information shared by you with HR Services or your manager (including relating to statutory and non-statutory leave types), performance information, and probation, disciplinary and grievances information, professional registration number, details of professional memberships, exit interview information (relating to the experience in the hospital and reason of leaving), details on secondments or temporary assignments and remote or flexible working arrangements (See [PPS-HR-046 - Flexible working policy](#)).

Special category data: We process the following special categories of personal data:

- Racial or ethnic origin, religious or philosophical beliefs or sexual orientation.
- Health information such as:
 - Occupational health referrals and reports
 - Sick leave forms or fit notes (i.e. Statement of Fitness for Work from a GP or Hospital)
 - Accident at work records (e.g. Risk Management)
 - Disability status, accessibility needs or reasonable adjustments
 - Health information (e.g. Department of Occupational Medicine)
- Trade union memberships.

Criminal offence data: We also process details of any criminal convictions (i.e. Garda Vetting Disclosures, overseas clearance) about you, as described in this notice. To comply with our legal obligations and to satisfy Garda Vetting requirements, the MMUH is required to process personal data relating to criminal convictions and offences.

How your personal data is collected

We typically collect personal data about employees, workers, contractors, and volunteers through the application and recruitment process, either directly from candidates or employees, or sometimes from an employment agency. If you are in any of these categories this notice applies to you. If you are employed as a contractor of MMUH through an employment agency or third party, please refer to the agency or third party notice also.

We will sometimes collect additional information about you from third parties, including former employers or other background check agencies, including, but not limited to:

- The Revenue Commissioners
- An Garda Síochána (Garda Vetting)
- Other Government Departments or State agencies, such as the Health Service Executive (HSE), Medical Council, CORU, NMBI
- Your doctor(s) or health professionals treating you
- Medical and occupational health professionals not employed by MMUH
- Educational institutions (for verification of qualifications and academic records)
- Professional licensing or regulatory bodies (for confirmation of credentials and professional standing, beyond those already listed)
- Referees provided by the candidates and references from these referees
- Internal records (such as previous employment history within MMUH, if applicable)
- Training providers (for verification of certifications or professional development courses)

Our legal basis for the collection and use of your data

Under the General Data Protection Regulation (GDPR), The Mater Hospital must have a legal basis for processing personal data.

Our legal bases for collecting or using your personal data are:

- **Contract** –We process your personal data in order to enter into, or fulfil, our employment contract with you; this processing is necessary for the performance of our contractual obligations and enforcement of our contractual rights. All of your data protection rights (refer to the section “Data Protection Rights” below) may apply, except the right to object. This processing is carried out in accordance with applicable data protection legislation and other relevant laws.
- **Legal obligation** –We are required to collect and further process your personal information in order to comply with our legal requirements and obligations, such as statutory enactments, regulatory obligations, or Court orders. This processing is necessary to ensure the Hospital meets its legal responsibilities under applicable law. In these circumstances, most of your data protection rights apply; however, please note that the right to erasure, the right to object, and the right to data portability may not apply when processing is based on a legal obligation. Further details regarding the statutory sources of our legal obligations can be found in the section “Key statutory obligations for processing information about you” below.
- **Public task** – We are required to collect and further process your personal information in order to tasks we carry out tasks in the public interest, as prescribed by law. This includes activities such as the management and provision of healthcare services, performance of our contract with the HSE, or the safeguarding or management of public revenues. Such processing is undertaken by organisations like ours, as mandated by legislation and we have set out below the primary laws that apply to us. In these circumstances, all of your data protection rights apply except for the right to erasure and the right to data portability, in accordance with the General Data Protection Regulation (GDPR) and relevant Irish and European laws.
- **Legitimate interests** – In certain limited circumstances, we may process your personal data where it is necessary to pursue the legitimate interests of our organisation, yourself, or a third party, provided these interests are not overridden by your own interests or fundamental rights and freedoms. Such processing is always separate to our public tasks and is carried out with careful consideration to ensure your rights are protected. Examples of legitimate interests include ensuring the security and safety of our staff, patients, and property (such as through the use of CCTV), and the planning, improvement, and management of our services where unrelated to our public tasks or role. We will only use your information for these purposes where it is appropriate and in accordance with data protection law. All of your data protection rights may apply, except the right to data portability.
- **Consent** – In certain limited circumstances, we may rely on your consent for the processing of personal data. For example, if your photograph is published on the Hospital website we will rely on your consent. All of your data protection rights apply.
- **Vital interest** – There can be rare occasions where it becomes necessary to use your personal data to protect your vital interests (or someone else’s vital interests) such as in an emergency situation. All of your data protection rights may apply, except the right to object and to portability.

Key statutory obligations for processing information about you

In accordance with the legal bases for processing personal data outlined above — namely, the performance of a contract, compliance with legal obligations, the execution of public tasks, the pursuit of legitimate interests, consent, and the protection of vital interests — the Mater Hospital is required to adhere to a range of statutory obligations. This section highlights some of the principal Irish and European legislation mandating the processing of your personal data, particularly where such processing is necessary to fulfil our public tasks and duties or meet legal requirements, including as prescribed in our contract with the HSE. For further information, you may consult the complete texts of these Acts and Statutory Instruments listed below on the [Irish Statute Book](#) and the [Houses of the Oireachtas](#) website.

- Adoptive Leave Acts 1995 and 2005;
- Automatic Enrolment Retirement Savings System Act 2024;
- Carer’s Leave Act 2001;
- National Cyber Security Act (on enactment);
- Disability Act 2005;
- Employment (Miscellaneous Provisions) Act 2018;
- Employment Equality Acts 1998 to 2021;
- European Communities (Protection of Employees on Transfer of Undertakings) Regulations 2003 (S.I. 131 of 2003);
- Health Act 2004 (in particular, section 38 and related service arrangements made between the HSE and the Mater Hospital under that section);
- Maternity Protection Acts 1994 to 2022;
- Minimum Notice and Terms of Employment Acts 1973 to 2005;
- NIS2 Directive (Directive(EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148);
- Organisation of Working Time Act 1997;
- National Minimum Wage Acts 2000 and 2015;
- National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016;
- Parental Leave Acts 1998 to 2023 and extension order 2024 (S.I. 92 of 2024);
- Parent’s Leave and Benefit Act 2019;
- Paternity Leave and Benefit Act 2016;
- Payment of Wages Act 1991;
- Pensions Acts 1990 to 2018;
- Protected Disclosures Act 2014;
- Protection of Employees (Part-Time Work) Act 2001;
- Protection of Employees (Fixed-Term Work) Act 2003;
- Protection of Employment Acts 1977 to 2024;
- Redundancy Payments Acts 1967 to 2014;
- Safety, Health and Welfare at Work Act 2004 to 2014;
- Sick Leave Act 2022;
- Social Welfare Acts;
- Taxes Consolidation Act 1997;
- Terms of Employment (Information) Acts 1994 to 2014;
- Unfair Dismissals Acts 1977 to 2015;

- Work Life Balance and Miscellaneous Provisions Act 2023;
- Workplace Relations Act 2015 (including the Workplace Relations Act 2015 (Fixed Payment Notice Regulations 2023 (S.I. 705 of 2023))).

(This list is not exhaustive and is subject to change as new or amended statutory and regulatory obligations are brought into force by the Oireachtas, European institutions and regulatory authorities)

How and why we process information about you

The purposes, and related legal bases and categories of personal data, for which we will process your personal data are listed in table below.

Recruitment and starting work

Purpose for which MMUH processes your personal data	Type of data (see section 'What information we process' above for further detail)	Legal basis upon which MMUH relies to process your personal data
<ul style="list-style-type: none"> • Making a decision about your recruitment or appointment. 	Identity data Contact details Recruitment data Employment data <i>If relevant and permitted by an additional ground (See "How we use your criminal offence data" below):</i> Criminal offence data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> • Checking you are legally entitled to work in Ireland. 	Recruitment data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> • Setting up your record in the HR Department 	Identity data Contact details Recruitment data Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See "How we use your special category data" below):</i> Health information	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> • Setting up your Records in the Salaries Department 	Identity data Contact details Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task

Administration and management including management of our working and contractual relationship

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> Determining the terms on which you work for us. 	Identity data Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> General administration of the employment contract we have entered into with you and any policies and procedures which apply to you from time to time. 	Identity data Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Business management and planning, including accounting and auditing. 	Identity data Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task Our legitimate interest in the planning, improvement, governance and management of our organisation, the services we provide, and our financial accountability, in activities other than those performing a public task.
<ul style="list-style-type: none"> Conducting performance reviews, managing performance and determining performance requirements. 	Identity data Contact details Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Assessing qualifications for a particular job or task, including decisions about promotions. 	Identity data Contact details Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work. 	Identity data Contact details Recruitment data Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See "How we use your special category data" below):</i>	Contract Legal Obligation Public Task

Purpose	Type of data	Legal basis
	Racial or ethnic origin, religious or philosophical beliefs or sexual orientation Health information Trade union membership <i>If relevant and permitted by an additional ground (See “How we use your criminal offence data” below):</i> Criminal offence data	
<ul style="list-style-type: none"> Gathering facts or evidence and any other steps relating to actual or possible grievance or disciplinary matters and associated hearings. 	Identity data Contact details Recruitment data Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See “How we use your special category data” below):</i> Racial or ethnic origin, religious or philosophical beliefs or sexual orientation Health information Trade union membership <i>If relevant and permitted by an additional ground (See “How we use your criminal offence data” below):</i> Criminal offence data	Contract Legal Obligation Public Task Our legitimate interest in the planning, improvement, governance and management of our organisation, the services we provide, and our financial accountability, in activities other than those performing a public task.
<ul style="list-style-type: none"> Making decisions about your continued employment or engagement. 	Identity data Contact details Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See “How we use your criminal offence data” below):</i> Criminal offence data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Making arrangements for the termination of our working relationship. 	Identity data Contact details Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See “How we use your criminal offence data” below):</i> Criminal offence data	Contract Legal Obligation Public Task Our legitimate interest in the planning, improvement and management of our service and administering our employment relationship with you

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> Education, training and development requirements. 	Identity data Contact details Recruitment data Employment data	Contract Legal Obligation Public Task Our legitimate interest in the planning, improvement, governance and management of our organisation, the services we provide, and our financial accountability, in activities other than those performing a public task.
<ul style="list-style-type: none"> To conduct data analytics studies to review and better understand employee retention and attrition rates. 	Identity data Contact details Recruitment data Employment data	Contract Legal Obligation Public Task Our legitimate interest in the planning, improvement, governance and management of our organisation, the services we provide, and our financial accountability, in activities other than those performing a public task.
<ul style="list-style-type: none"> To manage and deliver health services, including on behalf of the State and the HSE 	Identity data Contact details Recruitment data Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Dealing with Data Subject Access/ Freedom of Information Act/Environmental Information Regulations / other regulatory requests 	Identity data Contact details Recruitment data Employment data Financial and tax data	Contract Public task Legal obligation
<ul style="list-style-type: none"> Equal opportunities monitoring 	Identity data Contact details Recruitment data Employment data Financial and tax data <i>If relevant and permitted by an additional ground (See “How we use your special category data” below):</i>	Legal obligation (including to promote and support the employment persons with disabilities or under other protected grounds) Contract Public Task Our legitimate interest in the planning, improvement, governance and management

Purpose	Type of data	Legal basis
	Racial or ethnic origin, religious or philosophical beliefs or sexual orientation Health information	of our organisation, the services we provide, in activities other than those performing a public task.

Salaries and benefits

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> Paying you and, if you are an employee, deducting tax and PAYE, and other employee related deductions. 	Identity data Contact details Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Making decisions about salary reviews and compensation. 	Identity data Contact details Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Enrolling you into a pension scheme and liaising with your pension provider, providing information about changes to your employment such as promotions, changes in working hours. 	Identity data Contact details Employment data Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Verifying your eligibility for non-salary payments including discretionary payments (such as the 2022 Pandemic Special Recognition Payment (“PSRP”). 	Identity data Contact details Financial and tax data	Contract Legal Obligation Public Task
<ul style="list-style-type: none"> Recouping or rectifying overpayments of salaries, allowances or expenses made to you. 	Identity data Contact details Financial and tax data	Contract Legal Obligation Public Task

Monitoring

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> To monitor your business and personal use of our information and communication systems to ensure compliance with our IT policies. 	Identity data Contact details Employment data Monitoring data	Contract Legal Obligation Public Task Our legitimate interest to prevent fraud, security or data breaches, and to protect our systems, property, personnel and patients, in respect of activities other than those performing a public task or complying with a legal obligation.
<ul style="list-style-type: none"> To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. 	Identity data Contact details Employment data Monitoring data	Legal Obligation Public Task Our legitimate interest to prevent fraud, security or data breaches, and to protect our systems, property, personnel and patients, in respect of activities other than those performing a public task or complying with a legal obligation.
<ul style="list-style-type: none"> To ensure the safety and security of our physical premises. 	Monitoring data	Legal Obligation Public Task Our legitimate interest to prevent fraud, security or data breaches, and to protect our safety and security of our systems, property, personnel and patients, in respect of activities other than those performing a public task or complying with a legal obligation.

Staff health and well-being

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> Ascertaining your fitness to work, managing sickness absence. 	Identity data Contact details Employment data <i>If relevant and permitted by an additional ground (See “How we use your special category data” below):</i> Health Information	Contract Public task Legal obligation
<ul style="list-style-type: none"> Complying with health and safety obligations. 	Identity data Contact details Monitoring data Employment data <i>If relevant and permitted by an additional ground (See “How we use your special category data” below):</i> Health Information	Contract Public task Legal obligation

Administration of Hospital Information systems

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> User account creation and management for Hospital information systems 	Identity data Contact details	Contract Public task Legal obligation Our legitimate interest to prevent fraud, security or data breaches, and to protect our safety and security of our systems, property, personnel and patients, in respect of activities other than those performing a public task or complying with a legal obligation.
<ul style="list-style-type: none"> Access control and authentication 	Identity data Contact details Monitoring data	Contract Public task Legal obligation Our legitimate interest to prevent fraud, security or data breaches, and to protect our safety and security of our systems, property, personnel and patients, in respect of activities other than those performing a public task or

Purpose	Type of data	Legal basis
		complying with a legal obligation.
<ul style="list-style-type: none"> Monitoring system usage to ensure security and compliance 	Identity data System usage logs Device identifiers IP addresses	Contract Public task Legal obligation
<ul style="list-style-type: none"> Provision of IT support 	Identity data Contact details Support tickets Device information	Contract Public task Legal obligation Our legitimate interest in the management and delivery of our service in respect of activities other than those performing a public task or complying with a legal obligation.

Procurement, logistics [& marketing]

Purpose	Type of data	Legal basis
<ul style="list-style-type: none"> Managing procurement requests and approvals 	Identity data Contact details	Contract Public task Legal obligation Our legitimate interest in managing our service in a responsible and commercially prudent manner, in respect of activities other than those performing a public task or complying with a legal obligation.
<ul style="list-style-type: none"> Authorising purchases & expenditure 	Identity data Contact details	Contract Public task Legal obligation Our legitimate interest in managing our service in a responsible and commercially prudent manner, in respect of activities other than those performing a public task or complying with a legal obligation.
<ul style="list-style-type: none"> Communicating with suppliers and vendors 	Identity data Contact details	Contract Public task

Purpose	Type of data	Legal basis
		Legal obligation Our legitimate interest in managing our service in a responsible and commercially prudent manner, in respect of activities other than those performing a public task or complying with a legal obligation.

How we use your special category data

We only use your special category data when, in addition to having a legal basis that is required to process personal data (referred to previously in this Notice), there is an additional ground that permits us to do so. Those additional grounds include:

- **Employment and social welfare law:** When using your special category data is necessary for carrying out rights and obligations in connection with employment or social welfare law.
- **Legal rights, claims and proceedings:** When processing your special category data is necessary for the purpose of, or in connection with, any actual or prospective legal claims or proceedings, for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- **Health insurance and pension:** when using your special category data is necessary and proportionate for the purpose of a policy of insurance or life assurance or health or health-related insurance or pension arrangements.
- **Assessment of working capacity:** when using your special category data is necessary for the assessment of your working capacity by a health professional.
- **Public Health:** when using your special category data is necessary to protect against serious cross-border threats to health or ensure high standards of quality and safety of healthcare.

How we use your criminal offence data

We only process your criminal offence data when, in addition to one of the grounds that is required to process personal data (referred to previously in this Notice), there is a further ground that permits us to do so. The further grounds on which we may make use of criminal offence data include:

- **Consent:** Where you have given your explicit consent for us to process criminal offence data.
- **Employment:** When processing criminal offence data is necessary and proportionate for entering into or performing your employment contract.
- **Legal Obligation:** Where we are authorised or required by law to process criminal offence data.
- **Prevention of injury or damage:** Where it is necessary to prevent injury or other damage to you or anyone else, to protect your vital interest or those of another person, or to protect property from loss or damage.
- **Legal rights, claims and proceedings:** Where processing criminal offence data is necessary for the purpose of, or in connection with, any actual or prospective legal claims or proceedings,

for the purpose of obtaining legal advice, or is otherwise necessary for the purpose of establishing, exercising or defending legal rights.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated or new purpose to those set out in this Privacy Notice or otherwise outlined to you, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we will, if necessary, process your personal data without your consent, in compliance with the above rules, where this is required or permitted by law.

Your Data Protection Rights

It is important that the personal data we hold about you is accurate and up-to-date. Please keep us informed of any changes (e.g. change of name, address, next of kin, etc) during your working relationship with us.

Under the GDPR you have the following Rights:

- **Your right of access** - You have the right to ask us for copies of your personal data, where we get personal data from and who we share personal data with. There are some exceptions which means you may not receive all the information you ask for. You can read more about this right [here](#).
- **Your right to rectification** - You have the right to ask us to correct or delete personal data you think is inaccurate or incomplete. You can read more about this right [here](#).
- **Your right to erasure** - You have the right to ask us to delete your personal data under certain circumstances. You can read more about this right [here](#).
- **Your right to request restriction of processing** - You have the right to ask us to limit how we can use your personal data. You can read more about this right [here](#).
- **Your right to object to processing** - You have the right to object to the processing of your personal data where it based on the legal basis of legitimate interest or public task. You can read more about this right [here](#).
- **Your right to data portability** - You have the right to ask that we transfer the personal data you gave us to another organisation, or to you where the legal basis is consent or contract. You can read more about this right [here](#).
- **Your right to withdraw consent** – When you have consented to processing, you have the right to withdraw your consent at any time. Withdrawing your consent does not affect the lawfulness of processing based on consent before its withdrawal. You can read more about this right [here](#).

If employees have any queries in relation to the above, please contact the Data Protection Office or the Human Resources Department.

How long we keep information

The Mater Hospital will endeavour to only keep personal data for a period that is deemed necessary to carry out the function and operational purpose for which it was collected as outlined in this privacy notice, unless it is specifically required by law to keep your information for longer. All personal data is subject to a specified retention period in line with the Mater Hospital Record Retention Policy and the HSE Standards and Recommended Practices for Health Records Management and is securely destroyed once no longer needed.

For more information about how long we keep your information, take a look at our retention schedule online:

[Record Retention and Disposal Policy](#)

Who we share information with

In certain circumstances, we need to share your personal data with other parties:

- Training suppliers
- Internal and external auditors
- Professional advisors such as our legal advisors and other consultants (e.g. IBEC, etc.)
- Governmental, regulatory or law enforcement authorities where we are requested or required by law to do so such as: the Department of Health, the Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation, the Health Service Executive (HSE), the Health Information and Quality Authority (HIQA), the Medical Council, the Nursing and Midwifery Board of Ireland (NMBI), CORU, the Revenue Commissioners, and An Garda Síochána (e.g. for Garda Vetting).
- Courts, external investigators and the Workplace Relations Commission (WRC) in relation to grievances, disciplinary matters, disputes or claims.
- Providers of employment benefits and related schemes such as health insurers, CIE and Transport for Ireland regarding TaxSaver Leap Cards, participants in the bike-to-work scheme, etc.
- Academic and research institutions with whom we partner for research and education purposes.
- Sponsors, contract research organisations or other parties involved in health research.

In certain circumstances the Mater Hospital processes personal data on behalf of other organisations (such as the HSE according to its services arrangements under section 38 of the Health Act 2004) and that other organisation will be the controller of your data. For more information on how those organisations process your personal data, you should consult their privacy notices.

Data processors

We engage third parties to assist us with the delivery of some of our services or parts of them and in the activities that we carry out as a hospital. These are:

- Providers of services in relation to employment, recruitment and benefits.
- Providers of services supporting our IT systems, data and cloud storage, and security.
- Providers of laboratory and diagnostic services for the provision of our healthcare service.

Sharing information outside of Ireland

Where necessary, the Mater Hospital may share personal data outside of Ireland. When doing so, we comply with the GDPR, making sure appropriate safeguards are in place.

For further information or to obtain a copy of the appropriate safeguard for any of the transfers below, please contact us using the contact information provided above.

Organisation name: Allocate/Datix

Category of recipient: Data Processor

Country the personal data is sent to: United Kingdom

How the transfer complies with data protection law: Transfers on the basis of an [adequacy decision](#) issued by the European Commission under Article 45 of the GDPR.

Organisation name: Civica (formally Opas G2)

Category of recipient: Data Processor

Country the personal data is sent to: United Kingdom

How the transfer complies with data protection law: Transfers on the basis of an [adequacy decision](#) issued by the European Commission under Article 45 of the GDPR.

How to make a complaint?

You have the right to make a complaint if you are unhappy about how we hold, use or share your personal data. To make a complaint directly to the Hospital please contact the office below.

You also have a right to lodge a complaint with the data protection regulator, the Data Protection Commission (“DPC”) which can be contacted at:

Data Protection Commission

21 Fitzwilliam Square South

Dublin 2

D02 RD28

Ireland

Phone (01) 765 01 00

Freephone 1800 437 737

info@dataprotection.ie

Who to contact if you have any questions?

	Address	Phone	Email
Data Controller Mater Misericordiae University Hospital	Eccles St Dublin 7 D07 R2WY	+353 (01) 803 2000	ceooffice@mater.ie
Human Resources Department	Station Mews, Lindsay Grove, Dublin 9 D09 W8W8	+353 (01) 803 2686	humanresources@mater.ie
Data Protection Office	Eccles St Dublin 7 D07 R2WY	+353 (01) 803 4311	dataprotection@mater.ie

This Privacy Notice was last updated in February 2026 and may change from time to time. The most up-to-date copy will be available on the Mater Misericordiae University Hospital website or can be obtained by contacting the Data Protection Office (details above).



Data Protection

February 2026
Version 2.0