



POLICIES AND PROCEDURES

DOCUMENT DESCRIPTION

Status	Active
Number	GCH/MOI/POL/4
Title	Privacy and Personal Data Protection Policy
Type	Policy
Author	Data Protection Committee
Approved by	Chair, Data Protection Committee
Version	4
Active Date	July 1, 2023
Reviewed	February 1, 2024
Next Review Date	February 1, 2026
Accessed by	All Staff
Availability	Electronic copies
Custodian	Chair, Data Protection Committee

1. IMPORTANT INFORMATION

- 1.1. We are glad you are taking time to read the Gertrude's Children's Hospital's ("**Hospital**", "**we**", "**us**", "**our**") General Data Privacy Policy.
- 1.2. We respect your privacy and we are committed to processing personal data in accordance with the law and in particular, the Data Protection Act, 2019 (the "**Act**").
- 1.3. This Privacy Policy explains how we collect, use, share, and store (in other words, **Process**) personal data of third-party service providers (in the case of corporate entities, this refers to their individual representatives), potential employees seeking employment with us and, generally, members of the public (referred to as "**you**" or "**your**" in this Privacy Policy).
- 1.4. It is important that you read this Privacy Policy together with any other related privacy policy or privacy notice (**Other Privacy Documents**) we may provide from time to time, regarding Processing personal data about you (or personal data you provide), so that you are fully aware of how and why we are using such data. This Privacy Policy adds to such Other Privacy Documents and is not intended to override them.
- 1.5. Please note that we have a separate privacy policy for our patients, their families and other individuals who may use our healthcare services. Please contact us for a copy of such Policy.
- 1.6. We will regularly review this Privacy Policy. This version was last updated on February 2024.

2. WHO WE ARE

- 2.1. The Hospital is a "**data controller**" in relation to the Processing activities described below. This means that we determine the purpose and means of Processing your personal data (or personal data you provide).
- 2.2. The Hospital is registered as a "**data controller**" with the Office of the Data Protection Commissioner.
- 2.3. Our Data Processing Committee (DPC) is responsible for our data protection function. You can find contact details for our DPC team at the end of this Privacy Policy.

3. THE TYPES OF "PERSONAL DATA" THAT WE COLLECT AND PROCESS

- 3.1. "**Personal data**" means any information that can be used to identify an individual natural person. Please note that there are "special categories" of personal data that are more sensitive and require a higher level of protection. The personal data we collect will vary according to the circumstances surrounding our relationship with you.
- 3.2. We will collect, use, store, share or otherwise Process personal data about you (or persons connected to you) including:
 - 3.2.1. **Details about our third-party service providers:**
 - (a) **Personal details:** such as your name, date of birth, title, and job description, contact details such as your business email address, physical address and telephone number and other information required for Know Your Customer (KYC), Anti-Money Laundering (AML) and/or sanctions checking purposes (e.g., copies of your passport or a specimen of your signature).
 - (b) **Contractual details:** such as,
 - (i) information contained in your bids and/or your responses to our tenders or invitations,

- (ii) your written agreements/ contracts/ local purchase orders with us,
- (iii) signature authorizations issued by our corporate service providers,
- (iv) records relating to your performance in providing to us goods and services,
- (v) details of all invoices received from you (and associated purchase orders) as well as expenses claimed by you,
- (vi) details of payments to you, including records of associated taxes, details of your requests, queries, or complaints and
- (vii) bank account details insofar as our service provider is a nature person.

3.2.2. Details about applicants seeking employment with us:

- (a) **Personal details:** such as your name, title, gender, nationality, marital status, date of birth, place of birth, age, national identification/passport number, addresses, telephone numbers, personal email addresses, location data and details about your registration with any regulatory or professional body, credit background checks and any regulatory certificates and references.
- (b) **Recruitment details:** such as previous experience, skills, qualifications, references, interview and assessment data, background and verification data and other information included in a curriculum vitae/resume or cover letter or as part of the application process.

3.2.3. Details about members of the public:

- (a) **Personal details:** such as your name, title, gender, nationality, marital status, date of birth, place of birth, age, occupation, national identification/passport number, addresses, telephone numbers, personal email addresses and social media accounts.
- (b) **Hospital related details:** such as the purpose of contacting the Hospital including when inquiring about the Hospital's services or reporting a complaint, your responses to the Hospital's surveys or questionnaires and any health conditions when participating in any Hospital activities.
- (c) **Donation/ Fundraising related details:** such as the purpose of your donation, amount of your donation, where applicable the related organization making the donation and bank account details or any other payment method relating to your donation.

3.2.4. Details on our communication, marketing, and monitoring activities:

- (a) **Communications details:** such as information contained in voice, messaging, letter, email, and other communications we have with you. We may also keep records of our meetings and conversations whether with you or with other third parties about you or the good or services that you provide. Please note that as required and/or permitted by law, we also may monitor and record your telephone, email, instant messaging, and other online communications with us in connection with our Hospital operations.
- (b) **Monitoring information** such as:
 - (i) information about your use of our information and communications systems, including your website and system interaction (cookies, internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and similar technologies),
 - (ii) information about your use of the Hospital's facilities,
 - (iii) information about your interactions with us on social media,
 - (iv) information received in response to any surveys or complaint claims, and

- (v) information gathered through CCTV and building access information.
 - (c) **Marketing data:** such as your preferences for receiving marketing from us and our third parties and your communication preferences.
- 3.3. Please note that by providing us with any personal data about a third party, you will be confirming:
- (a) that you have obtained the necessary consent from those third parties to the use of their personal data, and
 - (b) that the third parties are aware of your actions.

4. **WHAT HAPPENS IF YOU FAIL TO PROVIDE THE REQUESTED PERSONAL DATA?**

If you do not provide us with the requested personal data needed for our operational purposes, we may not be able to appropriately provide you with the services you require or adequately assist you.

5. **HOW DO WE COLLECT YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)?**

- 5.1. We may collect or receive your personal data (or personal data you provide) in different ways:
- (a) Where you provide the personal data directly to us, for example:
 - (i) communicating with us by phone or email or social media,
 - (ii) participating in our tendering or recruitment processes,
 - (iii) participating in our surveys or questionnaires or research activity,
 - (iv) signing up to receive our marketing,
 - (v) during your relationship with us when accessing our services or when providing us with your goods or services,
 - (vi) completing a form, a security book, or events attendance lists to participate in events held by the Hospital), and
 - (vii) using or registering to use our website (i.e. <https://www.gerties.org/>). Please see section 9 on **Cookies** for further information.
 - (b) From third parties, such as your references, the business entities that you work for, your former colleges, former schools, and higher education institutions, regulatory or professional bodies and government departments/ agencies,
 - (c) From publicly available sources including but not limited to internet search engines, public records and registers and social media accounts (e.g., *Facebook, LinkedIn, and Twitter*),
 - (d) Where you provide the personal data indirectly to us through monitoring devices or by other means (for example, the Hospital's building and location access control and monitoring systems, CCTV, telephone logs and recordings, instant message logs and email and internet access logs), if and to the extent authorised by applicable laws.
- 5.2. Generally, you have no obligation to provide us with your personal data (or any person's personal data), but if you do not provide us with the information we need, we may be unable to appropriately provide you with services or assist you.
- 5.3. We will seek to minimise the amount of information we request for, to only that which is needed to perform the relevant function or service at the time.

6. HOW DO WE USE YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)?

6.1. We will store and Process your personal data (or personal data you provide) for any of the following purposes:

- (a) confirming your identity and communicating with you (or where applicable the corporate entity you are connected to),
- (b) managing and improving our relationship with you (or where applicable the corporate entity you are connected to),
- (c) making decisions about procuring your (or the related corporate entity's) goods and services including determining the terms of our contractual agreement,
- (d) undertaking contract, supply, and financial management, planning and reporting within our business,
- (e) enabling third parties to deliver products or services on our behalf, including I.T service providers,
- (f) managing, administering, and improving our business, client and service provider engagements and relationships and for corporate marketing, business development, analysis, and operational purposes,
- (g) evaluating recruitment applications for employment at the Hospital and undertaking pre-employment screening including, where relevant and appropriate, identity check, reference check, and criminal record checks,
- (h) operating security (including CCTV), governance, audit and quality assurance processes and arrangements,
- (i) fulfilling and monitoring our responsibilities under the various laws of Kenya,
- (j) enabling you to attend Hospital events, including fundraising activities,
- (k) communicating effectively with you by post, email, and phone, where appropriate you will be given the opportunity to opt-out of receiving some communications from us,
- (l) complying with our obligations to donors and sponsors (including our disclosure obligations under their terms and conditions and policies),
- (m) managing and maintaining your information in hard copy records, files, and systems, including technical support and maintenance of the Hospital systems and managing electronic and hard copy records in line with our retention schedules,
- (n) for business contingency planning and response to active incidents,
- (o) establishing, exercising and/or defending legal claims or rights and to protect, exercise and enforce our rights, property, or safety and those of our business, or any entity related to the Hospital,
- (p) investigating and responding to complaints or incidents relating to us or our business, to maintain service quality and to train staff to deal with complaints and disputes,
- (q) auditing, monitoring, investigation, and compliance monitoring activities in relation to our policies, codes of conduct, applicable law, the prevention, and detection of criminal activity and to protect our assets and premises,
- (r) meeting our obligations to, cooperating with, responding to requests from, complying with lawful requests by public authorities or where otherwise required or authorised by applicable laws, court orders, government regulations, or regulatory authorities (up to and including without limitation data protection, and tax), whether within or outside this country,

- (s) conducting compliance activities such as audit and reporting, assessing, and managing risk, maintenance of accounting and tax records, fraud, and anti-money laundering (AML) prevention and measures relating to sanctions and anti-terrorism laws and regulations and fighting crime,
- (t) recording and/or monitoring telephone conversations to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity. To the extent permitted by law, these recordings are our sole property,
- (u) for research and other statistical and trend analysis (de-identifying and aggregating or anonymizing source data with that of other clients and institutions in such way that it is not possible to reverse-engineer and re-identify you), and
- (v) complying with applicable laws and regulations.

7. LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)

7.1. We will only collect, use, and share your personal data (or personal data you provide) where we are satisfied that one of the following legal grounds apply to a specific Processing activity:

- (a) The Processing is necessary for the **performance of a contract** to which you are a party or to take steps, at your request, prior to entering such contract.
- (b) The Processing is necessary for the **legitimate interests** pursued by us or those of a third party to whom personal data is disclosed, except where such interests are overridden by your interests or rights and freedoms which require protection of personal data. We believe that we have a legitimate interest in Processing personal data for the purposes set out above, and to support the achievement of our immediate and long-term business goals and outcomes.
- (c) The Processing is necessary for us to comply with a **legal obligation** to which we are subject, for example, providing information on request to government entities or regulatory authorities; and conducting compliance activities such as audit and reporting, maintenance of accounting and tax records or anti-money laundering.
- (d) The Processing is based on your **consent**. We will rely on your consent as a lawful basis for Processing personal data, as appropriate, including the Processing of personal data relating to a child, Processing sensitive personal data outside Kenya, Processing your personal data for the purpose of direct marketing to you and where you have provided us with your consent.

Where you have provided your consent to the Processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific Processing at any time. Please note that by withdrawing your consent, the withdrawal will not render unlawful our prior Processing of your personal data or the Processing which is based on other legal bases for Processing of your personal data.

- (e) The Processing is necessary to **protect your interests** (or **someone else's interests**).
- (f) The Processing is necessary to perform a task carried out in the **public interest or for official purposes**.

7.2. Some of the above grounds for Processing will overlap and there may be several grounds which justify our use of your personal data (or personal data you provide).

8. CHANGE OF PURPOSE

- 8.1. We will use your personal data (or personal data you provide) solely for the purposes for which it was collected, unless we reasonably believe that we need to use it for another reason that is compatible with the original purpose.
- 8.2. If we need to use your personal data (or personal data you provide) for an unrelated purpose, we will notify you, explain our legal grounds for the change and obtain your consent to Process your personal data (or personal data you provide) for that unrelated purpose.
- 8.3. Please note that we may Process your personal data (or personal data you provide) without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

9. COOKIES

- 9.1. Please note that in order to improve our internet service to you, we will occasionally use a “cookie” and/or other similar technologies which may place certain information on your computer’s hard drive when you visit our website or any of the Hospital’s affiliated websites.
- 9.2. A cookie is a small amount of data that our web server sends to your web browser when you visit certain parts of our site.
- 9.3. We may collect cookies through, inter alia:
 - (a) information about your use of our services and about the device you use to access our services,
 - (b) the pages you request and visit and any posts you submit,
 - (c) information on your interaction with other pages,
 - (d) information obtained during maintenance or support of our website,
 - (e) information about your device such as MAC and IMEI numbers, your IP address, and the URLs of sites from which you arrive or leave our website, and
 - (f) your type of browser, your operating system, your mobile or internet service provider and the make and size of your device (such as for page displays and interoperability).
- 9.4. We use cookies to do many different jobs, like letting you navigate between pages efficiently, identifying you after you have logged in by storing a temporary reference number in the cookie, allowing you to access stored information if you register for any of our online platforms, and generally improving your online experience.
- 9.5. Cookies do not enable us to gather personal data about you unless you give the information to our server. Most Internet browser software allows the blocking of all cookies or enables you to receive a warning before a cookie is stored.

10. WHO DO WE SHARE YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE) WITH?

- 10.1. We will disclose your personal data (or personal data you provide) to any of the following as appropriate:
 - (a) our partner organisations,
 - (b) our external service providers where we outsource certain functions, including but not limited to, our IT and office systems, administrative services providers, and research companies. We will only disclose personal data to our external service providers when it

is essential for them to provide their service and we have a contract in place that requires them to keep your information secure and not to use it other than in accordance with our specific instructions,

- (c) funders and sponsors of the Hospital,
 - (d) our professional service providers (e.g., legal advisors, accountants, auditors, insurers and tax advisors),
 - (e) legal advisors, government and law enforcement authorities and other persons involved in, or contemplating, legal proceedings,
 - (f) competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction,
 - (g) other persons where disclosure is required by law or to enable products and services to be provided to you (or where applicable the corporate entity you are connected to),
 - (h) any other relevant professional or statutory regulatory bodies,
 - (i) establish, exercise, or defend our legal rights including providing information to others and/or in connection with any ongoing or prospective legal proceedings,
 - (j) prospective buyers as part of a sale, merger, or other disposal of any of our business or assets; and
 - (k) any other person you have authorised us by your consent to share your personal data with.
- 10.2. In all the cases cited above, we require all parties we share your personal data (or personal data you provide) with to respect the security of your personal data (or personal data you provide) and treat it in accordance with the law. Please note that we do not allow our external service providers to use your personal data (or personal data you provide) for their own purposes and only permit them to Process your personal data (or personal data you provide) for specified purposes and in accordance with our instructions.
- 10.3. Please note that if you request us, in writing, to share your personal data (or personal data you provide) with third parties, we will follow your request to share the relevant information. However, we do not have control over how those third parties will use your information. Before you make your request, we recommend that you (or the person acting on your behalf) consider the data protection practices of that third party by reading their privacy policies or contacting them.

11. CROSS BORDER TRANSFER OF PERSONAL DATA

- 11.1. We may transfer your personal data (or personal data you provide) to other hospitals, regulatory, prosecuting, tax and governmental authorities, courts and other tribunals, and other entities located in countries outside Kenya including countries which have different data protection standards to those which apply in Kenya.

12. DATA SECURITY

- 12.1. We have put in place appropriate physical and technical measures to safeguard your personal data (or personal data you provide) from being accidentally lost, used, or accessed in an unauthorised way.
- 12.2. For example, we will limit access to your personal data (or personal data you provide) to those employees, agents, contractors and other third parties that require it for legitimate business

purposes. They will only Process your personal data (or personal data you provide) on our instructions and they are subject to a duty of confidentiality.

- 12.3. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach if required by law.

13. THE RETENTION AND STORAGE OF YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)

- 13.1. We will only retain your personal data (or personal data you provide) for as long as necessary to accomplish the purposes for which it was collected, including complying with any legal, accounting, or reporting requirements.
- 13.2. We may retain your personal data (or personal data you provide) for a longer period if the retention is:
- (a) required or authorised by law,
 - (b) reasonably necessary for a lawful purpose,
 - (c) authorised or consented by you,
 - (d) for personal data that has been anonymised, or
 - (e) for historical, statistical, journalistic, literature and art or research purposes.
- 13.3. In some circumstances we may anonymise your personal data (or personal data you provide) so that it can no longer be associated with you, in which case we may use such information without further notice to you.

14. YOUR LEGAL RIGHTS

- 14.1. Subject to certain exceptions and limitations, you have a number of legal rights in relation to the personal data that we hold about you (or persons connected to you). These rights include the right to:
- (a) **be informed** of the use to which your personal data (or personal data you provide) is to be used,
 - (b) **request access** to your personal data (or personal data you provide) and receive a copy of the personal data we hold about you,
 - (c) **request correction and erasure** of the personal data that we hold about you,
 - (d) **request the restriction of Processing** of your personal data (or personal data you provide). This enables you to ask us to suspend the Processing of your personal data (or personal data you provide),
 - (e) **request us to transfer personal data** either to you or to another company in a commonly used electronic format. This is known as the right to data portability,
 - (f) **object to the Processing of your personal data (or personal data you provide)**,
 - (g) **object and opt-out** of our direct marketing services, and
 - (h) **request not to be subject to automated decision making**. This enables you to ask us not to make a decision about you that affects your legal position (or has some other significant effect on you) based purely on automated Processing of your data.

- 14.2. To exercise any of these rights, please write to our DPC via the contact details given below.
- 14.3. We will respond to your request without undue delay and no later than the time periods stipulated by the applicable Data Protection Legislation.

15. CONTACT US AND FURTHER INFORMATION

- 15.1. If you have any questions about this Privacy policy or how we handle your personal data (or personal data you provide), please contact dpc@gerties.org
- 15.2. We will respond to your questions and concerns in a timely manner and in compliance with the relevant laws.

16. CHANGES TO THIS PRIVACY POLICY

- 16.1. We reserve the right to update this Privacy Policy at any time and we shall notify you of the changes through electronic mail or such other means of communication which may be available to us.
- 16.2. We may also notify you in other ways from time to time about the Processing of your personal data (or personal data you provide).