Golders Hill Health Centre

Golders Hill Data Protection Policy

What is the GDPR?

The EU General Data Protection Regulation, or GDPR, is a significant enhancement to the old Data Protection Act 1998. This law aims to protect the personal data of individuals while that data is being used by various organisations.

Policy Statement

This Policy defines the responsibilities and expected behaviours of all our Employees, Contractors and relevant Organisation Partners which will uphold a Data Subject's right to have his or her Personal Data processed in accordance with the requirements of the GDPR.

This Policy applies to:

- the Personal Data of all Data Subjects with whom we interact during the normal course of our organisation
- all types of and uses for Personal Data within our organisation
- all our employees and organisation partners, especially those who deal directly with Personal Data
- all our organisation's processes and all systems (both manual and digital; internal and external) that process Personal Data
- all our data processing locations, whether in, or out of the country

What is Personal Data?

Personal data is information relating to an individual, including, but not necessarily limited to name, contact details, identity number, bank details, race, gender, age, health status, email address, location, online identifier and the like.
As an employee, you are a Data Subject and we use your Personal Data such as your name, identification, address and banking details; or perhaps sensitive data such as your health status or trade union membership. Our members are also Data Subjects as are the members of the Board of Governors, the Executive Committee and members of sub-committees, as well as any other individual's data we may process. The GDPR states that this Personal Data must be protected, and that Data Subjects must be able to access their Personal Data.

What are Special Categories of Personal Data?

This is sensitive information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or

data concerning a natural person's sex life or sexual orientation
What is a Data Subject?

A data subject is the identifiable, natural person to whom personal data belongs. For example, some of the data subjects of an organisation could be its customers and employees

What are the Rights of data subjects?

In order to protect the rights that the GDPR grants to data subjects, organisations need to observe the following:

- Every organisation is accountable for complying with the Regulation;
- Personal data may be collected and used only for specific and lawful purposes;
- Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which data is being processed;
- The personal data of children under 16 may only be collected and used upon consent of a parent or guardian;
- Personal data should not be retained for longer than is necessary for that specific purpose, and that information must be provided to the data subject;
- Where the personal data might be used for a purpose different to the original reason for collection, in most cases, the data subject's consent must be obtained;
- Personal data must remain accurate and up to date;
- Protect personal data from loss, theft and unauthorised access;
- Where personal data are processed by an external service provider (called a processor), ensure that contracts are in place which require that the processor also complies with these conditions;
- Where personal data is to be shared, ensure that there is a proper legal basis for sharing, and that the sharing is governed by a data sharing agreement;
- Have a system in place to notify the IC, and if necessary, the data subjects, of any breaches in security;
- Have a system in place to allow data subjects to exercise their rights to access and manage their personal data, and notify them of their right to do so;
- Data subjects may not be marketed to unless it is lawful to do so;
- Do not profile data subjects using purely automated means, (i.e. without human intervention) if your intention is to make any decisions which might significantly impact the data subject;
- Ensure that whenever consent is needed and given, that the consent is in writing and that you retain the evidence of consent having been given;
- Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement.

Golders Hill

Golders Hill Health Centre

What is a Controller?

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Our organisation is a controller.

What is a Processor?

The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, if our organisation were to outsource the processing of our payroll to an external organisation, that organisation would be the processor.

What is the Data Protection Policy?

The Data Protection Policy is internal to an organisation and demonstrates management's intent with regards to compliance with legislation such as the GDPR

What is a Privacy Notice?

A Privacy Notice draws special attention to the manner in which our organisation is complying with the GDPR. It is usually displayed at points where we collect personal data and informs data subjects as to their rights.

Certain information must be provided to the data subject at the time when their Personal Data is obtained.

Data Subject's Access to his or her Personal Data

Data subjects have the right to enquire whether an organisation holds their personal data and also to request the records or descriptions of those records. They have the right to challenge and even stop the processing of their personal data. They may request that their personal data be changed - e.g. where a name, surname or contact details change. When a data subject makes a request for access, the data subject's identity must be confirmed before you may continue with the response. GDPR365, our data protection management system, has a special section to assist with data subject access management. If you recognise a request for information you need to alert your manager.

Golders Hill

Golders Hill Health Centre

How do I play my part in protecting Personal Data?

Understand and respect the rights of data subjects

Be aware that some information within our organisation is classified as ‘Confidential’ and must be treated accordingly

All personal data in our organisation is classified as ‘Confidential’

Understand what we mean by the ‘Acceptable Use’ of our digital systems

Use strong passwords and keep them to yourself

Understand how to recognise suspicious emails and links

Think twice before clicking on any suspicious links

Keep your workstation clear

Practice discretion when you are outside and discussing our organisation

Keep our IT equipment safe, especially when you are outside the organisation premises

Be aware of the limitations we set with regards internet access and usage

If you know your rights as a data subject, it will be much easier for you to apply this knowledge in the execution of your own job.