

Policy statement

Pilgrim Hospital Radio is committed to protecting personal data and respecting the rights of our data subjects – the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

- a. maintain our lists of members, volunteers and supporters;
- b. provide our services within the local community
- c. safeguard children, young people and adults at risk;
- d. recruit, support and manage volunteers;
- e. maintain our accounts and records;
- f. promote our services;
- g. raise funds;
- h. respond effectively to enquirers and handle any complaints.

This policy has been approved by the Trustees who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

Why this policy is important

We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

This policy sets out the measures we are committed to taking as an organisation and, what each of us will do to ensure we comply with the relevant legislation.

In particular, we will make sure that all personal data is:

- a. processed lawfully, fairly and in a transparent manner;
- b. processed for specified, explicit and legitimate purposes, and not in a manner that is incompatible with those purposes;
- c. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- d. accurate and, where necessary, up-to-date;
- e. not kept longer than necessary for the purposes for which it is being processed;
- f. processed in a secure manner, by using appropriate technical and organisational means; and
- g. processed in keeping with the rights of data subjects regarding their personal data.

HBA - supporting Hospital Broadcasting in the UK

For more information see www.hbauk.com, e-mail info@hbauk.com, or call 0300 121 0500.

HBA is the operating name of the National Association of Hospital Broadcasting Organisations.
Registered in England and Wales as a company limited by guarantee (No. 2750147) and a charity (No. 1015501).
Registered Office: Avebury House, St Peter Street, Winchester, SO23 8BN

Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

Data subjects include all living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

- a. our volunteers (and potential and former volunteers);
- b. trustees;
- c. patients;
- d. programme contributors;
- e. members of staff at United Lincolnshire Healthcare Trust (Hereafter ULHT) and other partner organisations;
- f. supporters;
- g. enquirers;
- h. complainants;
- i. friends and family;
- j. representatives of other organisations.

ICO means the Information Commissioner's Office, the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special categories of data (as identified in the GDPR) includes information about a person's:

- a. Racial or ethnic origin;
- b. Political opinions;
- c. Religious or similar (e.g. philosophical) beliefs;
- d. Trade union membership;
- e. Health (including physical and mental health, and the provision of health care services);
- f. Genetic data;
- g. Biometric data;
- h. Sexual life and sexual orientation.

How this policy applies to you

As a trustee or volunteer processing personal information on behalf of Pilgrim Hospital Radio, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact the Chairman/Vice Chairman immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

As a team leader: You must make sure that any procedures in your area that involve personal data follow the rules set out in this Data Protection Policy.

As a data subject of Pilgrim Hospital Radio: We will handle your personal information in line with this policy.

Before you collect or handle any personal data as part of your voluntary work for Pilgrim Hospital Radio, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Chairman/Vice Chairman.

Training and guidance

We will provide general training at least annually for all volunteers to raise awareness of their obligations and our responsibilities, as well as to outline the law.

We might also issue procedures, guidance or instructions from time to time. Team leaders must set aside time for their team to look together at the implications for their work.

Our data protection responsibilities

What personal information do we process?

In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive directly from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, references for volunteers and requests and dedications for patients.

We process personal data in both electronic and paper form; all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, music requests, donations they have made to Pilgrim Hospital Radio and visual images of people.

In some cases, we hold types of information that are called “special categories” of data in the GDPR. This personal data can only be processed under strict conditions.

‘Special categories’ of data (as referred to in the GDPR) includes information about a person’s: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is an overarching safeguarding requirement to process this data for the protection of children and adults who might be put at risk by our work.

Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

Processing of personal data is only lawful if at least one of the following legal conditions, as set out in the GDPR, is met:

- a. the processing is necessary for a contract with the data subject;
- b. the processing is necessary for us to comply with a legal obligation;
- c. the processing is necessary to protect someone’s life (this is called “vital interests”);
- d. the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
- e. the processing is necessary for legitimate interests pursued by Pilgrim Hospital Radio or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject; or
- f. if none of the other legal conditions apply, the data subject has given their clear consent.

How can we legally use ‘special categories’ of data?

Processing of ‘special categories’ of personal data is only lawful when, in addition to the conditions above, one of the additional conditions, as set out in the GDPR, is met. These conditions include where:

- a. the processing is necessary for carrying out our obligations under employment and social security and social protection law;
- b. the processing is necessary for safeguarding the vital interests of an individual and the data subject is incapable of giving consent;
- c. the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
- d. the processing is necessary for pursuing legal claims, or
- e. if none of the other legal conditions apply, the data subject has given their explicit consent.

What must we tell individuals before we use their data?

If personal data is collected directly from the individual, we will inform them about our identity/contact details, the reasons for processing and the legal bases, where relevant explain our legitimate interests and/or the consequences of not providing data needed for a contract or statutory requirement, who we will share the data with, if we plan to send the data outside of the European Economic Area; how long we will store the data, and their data subjects’ rights.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described above as well as the source of the data. This information will be provided to the individual, in writing, no later than within 1 month after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Pilgrim Hospital Radio, we will give the data subject this information before we pass on the data.

When we need consent to process data

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

Processing for specified purposes

We will only process personal data for the specific purposes explained in our privacy notices (see "What must we tell individuals before we use their data?" above) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects, by providing them with updated privacy notices, unless there are lawful reasons for not doing so.

Data will be adequate, relevant and not excessive

We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data "just in case" we want to process it later.

Accurate data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

Keeping data and destroying it

We will not keep personal data longer than is necessary for the purposes that it was collected for.

Security of personal data

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing. Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

- a. the quality of the security measure;
- b. the costs of implementation;
- c. the nature, scope, context and purpose of processing;

- d. the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
- e. the risk which could result from a data breach.

Measures may include:

- a. technical systems security;
- b. measures to restrict or minimise access to data;
- c. measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- d. physical security of information and of our premises;
- e. organisational measures, including policies, procedures, training and audits;
- f. regular testing and evaluating of the effectiveness of security measures.

Keeping records of our data processing

To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

Working with people we process data about (data subjects)

Data subjects' rights

We will process personal data in line with data subjects' rights, including their right to:

- a. request access to any of their personal data held by us (known as a 'Subject Access Request');
- b. ask to have inaccurate personal data changed;
- c. restrict processing, in certain circumstances;
- d. object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
- e. data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;
- f. not be subject to automated decisions, in certain circumstances; and
- g. withdraw consent when we are relying on consent to process their data.

If any volunteer receives any request from a data subject that relates, or could relate, to their data protection rights, this must be forwarded to the Chairman/Vice Chairman immediately.

We will act on all valid requests as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully, extend the timescale. This can be extended by up to two months in some circumstances.

All data subjects' rights are provided free of charge.

Any information provided to data subjects will be concise and transparent, using clear and plain language.

Direct marketing

We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around direct marketing. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, and telephone.

Direct marketing means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be

advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

Any direct marketing material that we send will identify Pilgrim Hospital Radio as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

Working with other organisations and transferring data

Sharing information with other organisations

We will only share personal data with other organisations or people when we have a legal basis to do so, and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed Trustees are allowed to share personal data.

We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied.

Data processors

Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Transferring personal data outside the European Economic Area (EEA)

Personal data cannot be transferred (or stored) outside of the European Economic Area unless this is permitted by the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EEA.

We will only transfer data outside the EEA where it is permitted by one of the conditions for non-EAA transfers in the GDPR, such as when the recipient is certified under the US "Privacy Shield" scheme.

Managing change & risks

Data protection impact assessments

When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO.

DPIAs will be conducted in accordance with the ICO's Code of Practice.

Dealing with data protection breaches

Where volunteers think that this policy has not been followed, or data might have been breached or lost, this must be reported immediately to the Chairman/Vice Chairman

We will keep records of personal data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when someone in Pilgrim Hospital Radio becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.