Bath Institute for
Rheumatic Diseases

# BIRD Data Management Policy

- Policy prepared by the Executive Director
- Approved by Council of Management on 5 June 2018
- Policy became operational on 22 May 2018
- Next review date: September 2018 and then April 2019

## 1. Context and overview

BIRD needs to gather and use certain information about individuals.

These can include customers, suppliers, event attendees, contractors, trustees, volunteers, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the BIRD's data protection standards – and to comply with the law.

**Why this policy exists:**

This data management policy ensures BIRD:

- Complies with data protection law and follows good practice
- Protects the rights of customers, contractors, volunteers, staff and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

**Data protection law:**

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

## 2. Who? People and responsibilities

Everyone at BIRD contributes to compliance with GDPR. Key decision makers must understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance.

Here the key areas of responsibility are assigned:

- Keeping trustees updated about data protection issues, risks and responsibilities – **Executive Director**
- Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule – **Executive Director**
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each area that processes personal data. The policies themselves will stand as proof of compliance. – **Executive Director**
- Dissemination of policy across the organisation, and arranging training and advice for staff – **Executive Director**
- Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters - **Administrator**
- Checking and approving contracts or agreements with third parties that may handle the organisation's sensitive data – **Administrator**
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards - **Administrator**

- Performing regular checks and scans to ensure security hardware and software is functioning properly - **Administrator**
- Evaluating any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations – **Administrator**
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to BIRD's use of their data – **Executive Director**
- Ensuring that communications, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles – **Executive Director**

**Data Protection Officer (DPO) –** BIRD is not required in law to appoint one, but the person responsible for fulfilling the following tasks in respect of BIRD is the Executive Director, Celia Mead.

- To inform and advise the organisation and its employees/contractors about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities
- Note that the first point of contact for individuals whose data is processed (employees, customers etc) it is the Administrator

## 3. Scope of personal information to be processed

We process the following:

  - names of individuals
  - postal addresses of individuals
  - email addresses
  - telephone numbers
  - online identifiers (cookies, internet protocol addresses)
  - individual's disease conditions (for patient engagement newsletters and invitations to info days)
  - donations received from individuals
  - event attendance
  - trustee dates of birth, countries of birth and employer for investment due diligence (avoidance of money laundering)
  - photographs of individuals, together with their model release statements
- the data is collected from their responses and and stored only on BIRD's drives or paper filing
- we ensure that the data is accurate by contacting individuals for consent, by using NHS R&D mailing service (for disease types) to send invitations. Every 3 years, we review the accuracy of our lists by mailing contacts, this will next **fall**

**due in May 2021**. Every year we review the file records we keep and dispose of those we no longer need.

- we hold details of sensitive special categories of personal information, in particular names and addresses of patients who suffer from rheumatic diseases, at least one type of which is fatal in a few cases. The enhanced measures that are set in place to protect this information are password protected lists only on our system which only the administrator can access. We will no longer hold such data on cloud storage.

## 4. Uses and conditions for processing

We have conducted a full audit of all information we process and we keep evidence of consent to demonstrate that it is freely and unambiguously given for our specific purposes, and that data subjects can reasonably understand who we are and how we are using their information and allows them to state the preferred communications channels.

We communicate an individual's right to withdraw consent at any time, and do our processes and systems support the functionality to do so.

We notify the customer of their right to unsubscribe with every communication.

## 5. Privacy Impact Assessments

We are concerned with the type of privacy known as privacy of personal information. We will use PIA s to help us identify and minimise the data protection risks of new projects, as part of data protection by default and by design approach. This will include a description of the processing operations and the purposes and an assessment of the risks to individuals.

## 6. Data Sharing

We will not sell personal information to any third party organisations. We may share personal information to third party service providers who help us to process information, specifically MailChimp, SurveyMonkey and Google Analytics.

## 7. Security measures

Here are the measures that are in place to protect the personal information we store from breach:

- All personal data must only be stored only on BIRD's system
- All personal data must be deleted from home or non-BIRD systems, including Dropbox and cloud storage
- All computers owned by BIRD must have a PIN number and be password protected

- Any computers or mobile phones used for BIRD work but not owned by BIRD (in the case of contractors) must use a PIN number or password for access
- Third party distributors (eg Mailchimp, SurveyMonkey, Paperless Post) must meet GDPR standards

If any member of the team believes there has been a breach, they must notify the Executive Director immediately. The ED will then notify the ICO; consider whether to notify customers; and record details in our own breach log.

The essential facts must be recorded:

- the name and contact details
- the date and time of the breach (or an estimate)
- the date and time you detected it
- basic information about the type of breach
- basic information about the personal data concerned

We will delete data, including from browser history, and without further risk of breach.

## 8. Subject access requests

All individuals who are the subject of data held by BIRD are entitled to:

- Ask what information BIRD holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date and that we will check every 3 years
- Be informed how BIRD is meeting its data protection obligations

BIRD will fulfil subject access requests by establishing ID. In the case of patients, using higher level ID (photo ID, in the form of passport or driving licence). BIRD will charge £10 to fulfil the request. BIRD may ask for information to assist in locating the data. Individuals will be notified of this process by phone, email or letter.

Where a partner makes a request, we require written consent from the patient and photo ID from both, or a death certificate of the patient and photo ID of the partner.

## 9. The right to be forgotten

All patients have the right to be deleted from our database. Names, contact details and any correspondence would be deleted at their request.

Numbers of patients by disease areas might be retained, and other anonymous quantitative data, but only where no individual is identifiable.

In other cases, such as previous contractors or trustees, we would evaluate the right, and as long as it were legal (in terms of reporting to, say, tax authorities) we would delete their details.

## 10. Privacy notices

BIRD aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights.

To these ends the organisation has a privacy statement, setting out how data relating to these individuals is used by the company.

The privacy statement can be viewed by individuals on BIRD's website and is linked to in all consent requests

## 11. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. BIRD details here the ongoing measures implemented to:

1) Maintain evidence of the privacy measures implemented and records of compliance – see audit. This will be re-run every 3 years, next due in May 2021
2) Regularly test the privacy measures implemented and maintain records of the testing and outcomes – see consent mail out evidence May 2018.
3) Keep records showing training of employees on privacy and data protection matters – see training record

**Ongoing review**

This will be necessary whenever any changes occur to personnel, practices or policies, or technical infrastructure that impact any of the information given.

A formal date for holistic review is given in section 1, but the document should be considered a dynamic articulation of the organisations data management policy which is under constant revision.