# EXETER PRIDE

# POLICY COVERSHEET

| | |
|---|---|
| **Name of Policy:** | GDPR Policy |
| **Owner and key contacts:** | Data Protection Officer |
| **Date issued:** | January 2024 |
| **Purpose of Policy:** | • To protect the privacy individuals and their data who engage with Exeter Pride.<br>• To explain the responsibilities Exeter Pride and its members, volunteers and trustees have in respect to data.<br>• To provide members of Exeter Pride with information regarding GDPR, data and how to protect it.<br>• To explain how Exeter Pride collects, stores and uses data in compliance with GDPR.<br>• To provide a clear procedure to be implemented in the case of a data breach |
| **Intended Audience(s):** | Trustees, Committee, Members and Volunteers, wider public |
| **Approval for this Policy given by:** | Trustee Board |

| **Version Control** | | | |
|---|---|---|---|
| **Current Version Number** | 2.0 | | |
| **Date of Last review** | February 2025 | | |
| **Date of Next review** | February 2028 | | |
| **Expiry date** | *The policy is reviewed triennially* | | |
| **Amendment History** | | | |
| ***Ensure links are updated online following amendments.*** | | | |
| **Version No.** | **Date** | **Summary of amendments (if no change, write NA)** | **Author** |
| 1.0 | Jan 24 | N/A Policy Created | Annie Bennett |
| 2.0 | Feb 25 | Policy first review. Review to be triennially going forward | Annie Bennett |

## INTRODUCTION

Exeter Pride aims to ensure that all personal data collected about trustees, members, volunteers and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format. Exeter Pride is also committed to proactively protecting all data gathered and storing said data securely. Exeter Pride is committed to ensuring all data subjects are fully informed about how their data will be collected, stored and used. Exeter Pride is fully committed to reporting any data breaches immediately.

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

## DEFINITIONS

| **Term** | **Definition** |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| Special categories of personal data | Personal data, which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Principles<br>• Religious or philosophical beliefs<br>• Health – physical or mental<br>• Sex life or sexual orientation<br>• Sensitive personal data does not include data about criminal allegations, proceedings or convictions. Such data would not be gathered with the exemption of DBS checks for Trustees and Board Members. |

| | |
|---|---|
| | In the case of criminal offence (DBS) data, Exeter Pride is only able to process this if it is either:<br>• Under the control of official authority;<br>• or Authorised by domestic law.<br><br>The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the following conditions: The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health and research. |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

The key objectives of this policy are:

- To protect the privacy individuals and their data who engage with Exeter Pride.
- To explain the responsibilities Exeter Pride and its members, volunteers and trustees have in respect to data.
- To provide members of Exeter Pride with information regarding GDPR, data and how to protect it.
- To explain how Exeter Pride collects, stores and uses data in compliance with GDPR.
- To provide a clear procedure to be implemented in the case of a data breach.

## THE DATA CONTROLLER

Exeter Pride processes personal data relating to Trustees, Committee Members, volunteers and others and therefore is a data controller.

## ROLES AND RESPONSIBILITIES

This policy applies to all Trustees, Committee Members and Volunteers. Anyone who does not comply with this policy may face disciplinary action.

## BOARD OF TRUSTEES

The Board of Trustees has overall responsibility for ensuring that Exeter Pride complies with all relevant data protection obligations.

## DATA PROTECTION OFFICER

- The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, developing related policies and guidelines where applicable and carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.
- They will provide an annual report of their activities to the Trustee Board and, where relevant, report to the Board their advice and recommendations on data protection issues.
- The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
- Our DPO is Annie Bennett and is contactable via a.bennett@exeterpride.co.uk

## RESPONSIBILITIES

Exeter Pride acknowledges that GDPR is everyone's responsibility, and all Trustees, Committee Members and Volunteers will agree and adhere to Exeter Pride's GDPR and Privacy policy.

Exeter Pride has a trained Data Protection Officer (DPO) who has day-to-day responsibility over GDPR and Privacy procedure and will ensure the proper implementation of the Policy and adherence by all members to this. The DPO must be a Committee Member and have sufficient training, or be in the process of receiving such training, to carry out their duties. The DPO has a duty to report serious incidents to the relevant regulatory bodies in consultation with the Trustees, to ensure accurate and secure record keeping and up-to-date training of Trustees, Committee Members and Volunteers.

## TRUSTEES

Trustees have a legal responsibility to comply with the Charity's governing documents, to work in the best interests of the charity, to ensure the Charity is carrying out its purpose for public benefit and to hold the Charity accountable. This includes ensuring adherence to the GDPR policy. Trustees will consult with the Data Protection Officer if a data breach has arisen (or there is an identifiable risk that a breach many occur or storage is insecure) and support them in making the necessary referrals to Information Commissioners Office (ICO).

## COMMITTEE MEMBERS, TRUSTEES & VOLUNTEERS

All Trustees, Committee Members and Volunteers agree to adhere to the Charity's GDPR policy and undertake necessary training. Trustees, Committee Members and Volunteers will report all data breaches to the DPO at the earliest opportunity.

All Trustees, Committee Members and Volunteers will have agreed to the Safeguarding Policy and Safeguarding Code of Conduct which includes key information regarding GDPR.

## LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Consent: where the data subject has given clear consent for Exeter Pride to process their personal data for a specific purpose. Consent means offering people genuine choice and control over Exeter Pride uses their data. The UK GDPR builds on the 1998 Act standard of consent in several areas and contains much more detail:

**Exeter Pride will:**

- keep **consent requests prominent and separate from other terms and conditions.**
- Seek **a positive opt-in** such as unticked opt-in boxes or similar active opt-in methods.
- Avoid making consent a precondition of service.
- Be specific and granular. Allow individuals to consent separately to different purposes and types of processing wherever appropriate.
- **Keep records of what an individual has consented to, including what Exeter Pride told them, and when and how they consented**.
- **Tell individuals they can withdraw consent at any time and how to do this.**

**Right to be informed including privacy information**

- Individuals need to know that Exeter Pride are collecting their data, why you are processing it and who you are sharing it with.
- Exeter Pride publishes this privacy information on our website and within any forms or letters Exeter Pride sends to individuals. The information must be:
  concise, transparent, intelligible and easily accessible; written in clear and plain language and free of charge.

**Right to request data by individuals (Subject Access request).**

- Individuals have the right to obtain:
- confirmation that Exeter Pride are processing their data;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.
- Individuals can request information verbally or in writing. Exeter Pride must provide a copy of the information free of charge.
- However, Exeter Pride can charge a 'reasonable fee' when a request is: manifestly unfounded or excessive, particularly if it is repetitive, unless Exeter Pride refuse to

respond; or for further copies of the same information (that's previously been provided). This does not mean that Exeter Pride can charge for all subsequent access requests.

- Exeter Pride must base the fee on the administrative cost of providing the information.
- Exeter Pride must provide information without delay and at least within one calendar month of receiving it. Exeter Pride can extend this by a further two months for complex or numerous requests (in which case Exeter Pride must inform the individual and give an explanation).
- Exeter Pride should calculate the time limit from the day Exeter Pride received the request (whether the day is a working day or not) until the corresponding calendar date in the next month. A calendar month ends on the corresponding date of the next month (eg 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (eg 31 January to 28 February).
- If the corresponding date falls on a weekend or a public holiday, Exeter Pride has until the next working day to respond (e.g. Exeter Pride receives a request on 31 March. As there is no equivalent date in April, Exeter Pride has until 30 April to respond. However, if 30 April falls on a weekend, or is a public holiday, you have until the end of the next working day to respond).
- This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes if a consistent number of days is required (e.g. for a computer system), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.
- Exeter Pride must verify the identity of the person making the request, using "reasonable means".
- If the request is made electronically, Exeter Pride should provide the information in a commonly used electronic format.

**Right to erasure / restriction of data.**

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary for the purpose Exeter Pride originally collected/ processed it for;
- the individual withdraws consent;
- Exeter Pride are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- Exeter Pride are processing the personal data for direct marketing purposes and the individual objects to that processing;
- it was unlawfully processed (i.e. otherwise in breach of the UK GDPR);
- it has to be erased in order to comply with a legal obligation; or
- it is processed for information society services to a child.

Individuals can make a request for erasure verbally or in writing. Exeter Pride must verify the identity of the person making the request, using “reasonable means”.

Exeter Pride should respond to a request without delay and at least within one month of receipt. Exeter Pride should calculate the time limit from the day Exeter Pride receives the request (whether the day is a working day or not) until the corresponding calendar date in the next month. A calendar month ends on the corresponding date of the next month (e.g. 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).

If the corresponding date falls on a weekend or a public holiday, Exeter Pride have until the next working day to respond (e.g. Exeter Pride receives a request on 31 March. As there is no equivalent date in April, Exeter Pride has until 30 April to respond. However, if 30 April falls on a weekend, or is a public holiday, Exeter Pride has until the end of the next working day to respond).

This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes if a consistent number of days is required (e.g. for a computer system), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Exeter Pride can extend this period by a further two months for complex or numerous requests (in which case Exeter Pride must inform the individual and give an explanation).

Exeter Pride can refuse to comply with a request for erasure if Exeter Pride are processing the personal data for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- to perform a public interest task or exercise official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- to exercise or defence of legal claims;
- for public health purposes in the public interest; or
- for processing that is necessary for the purposes of preventive or occupational medicine, if you are processing the data by or under the supervision of a health professional.

A written retention policy or schedule will remind Exeter Pride when to dispose of various categories of data and help Exeter Pride plan for its secure disposal.

Exeter Pride will regularly review our retention schedule to make sure it continues to meet charity and statutory requirements and agree any amendments with DPO and Trustees and committee members and incorporate them into the new schedule.

Exeter Pride designates responsibility for retention and disposal to the DPO.

**Individuals have a right to block or restrict the processing of their personal data. (see above for procedure).**

As a matter of good practice, Exeter Pride will restrict the processing of personal data if:

- an individual contests the accuracy of the personal data. Exeter Pride will restrict the processing until the accuracy of the personal data is verified.
- an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and Exeter Pride is considering whether the charity's legitimate grounds override those of the individual.
- processing is unlawful and the individual opposes erasure and requests restriction instead.
- Exeter Pride no longer needs the personal data, but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim.

**Establishing, reviewing and updating Privacy Policy including GDPR compliance.**

- Exeter Pride had created a Privacy Policy in line with UK GDPR policy and principles. This policy will help Exeter Pride address data protection in a consistent manner and demonstrate accountability under the UK GDPR. This is a standalone policy statement that intersects with Exeter Pride's overall GDPR policy.
- The Privacy Policy clearly sets out Exeter Pride's approach to data protection together with responsibilities for implementing the policy and monitoring compliance.
- Trustees and committee members will approve the policy and publish and communicate it via Exeter Pride's website. Exeter Pride Trustees and Committee Members will review and update the policy annually or when required to ensure it remains relevant.

**GDPR and data handling training.**

- Exeter Pride will brief all staff handling personal data on their data protection responsibilities. Exeter Pride will provide **awareness training** on or shortly after appointment with updates at regular intervals or when required.
- Exeter Pride will also consider **specialist training** for staff with specific duties, such as information security and database management and marketing.
- DPO will regularly communicate key messages to reinforce training and maintain awareness (for example intranet articles, circulars, team briefings and posters).

**Security & breach policy.**

- All Exeter Pride's IT systems and data storage systems need to be safe and secure. This must include; password protection and 2 factor authentication. No paper records are to be printed or held. Any currently held must be shredded and disposed of via secure destruction of data processes.
- Exeter Pride Trustees and Committee Members processing personal data within IT system need to recognise the risks involved and take appropriate technical and organisational measures to secure the data.
- All communications / records to be kept on Exeter Pride emails, TEAMS and secured WhatsApp group.

**BREACH: Overall guidance.**

- The UK GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.
- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Exeter Pride have to notify the ICO of a breach unless it is unlikely to result in a risk to the rights and freedoms of individuals.
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Exeter Pride must notify those concerned directly and without undue delay.
- In all cases Exeter Pride must maintain records of personal data breaches, whether they are notifiable to the ICO.
- Exeter Pride must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The UK GDPR recognises that it will not always be possible to investigate a breach fully within that time-period and allows Exeter Pride to provide additional information in phases, so long as this is done without undue further delay
- Exeter Pride should make sure that Trustees and Committee Members understand what constitutes a personal data breach, and that this is more than a loss of personal data.
- Exeter Pride's internal breach reporting procedure are outlined below
- In light of the tight timescales for reporting a breach - it is important that Exeter Pride have robust breach detection, investigation and internal reporting procedures in place.

**BREACH: Specific actions / guidance.**

- On finding or causing a breach, or potential breach, the data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred.
  - To decide, the DPO will consider whether personal data has been accidentally or unlawfully: Lost, Stolen, Destroyed, Altered, Disclosed or made available where it should not have been, Made available to unauthorised people.

- The DPO will alert the Trustees and Committee Members.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through: loss of control over their data, discrimination, identity theft or fraud, Financial loss, Damage to reputation, Loss of confidentiality, any other significant economic or social disadvantage to the individual(s) concerned If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on Exeter Pride's secure TEAMS area.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out: a description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO.
For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored

The DPO and Trustees and Committee Members will meet as soon as possible to review events and agrees preventative strategies for the future.

**Actions to minimise the impact of data breaches.**

- Exeter Pride will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information.
- Exeter Pride will review the effectiveness of these actions and amend them as necessary after any data breach.

**Sensitive information being disclosed via email (including safeguarding records).**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Those who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure Exeter Pride receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, Exeter Pride will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.