The Phoenix Fellowship Privacy Policy

Version: 1.0

Introduction and purpose

The Phoenix Fellowship respects the privacy of every person who applies to us, engages with us, donates to us, partners with us, works or volunteers with us, or visits our website. This Privacy Policy explains, in clear terms, what personal information we collect, why we collect it, how we use it, who we share it with, how long we keep it, and how you can exercise your data protection rights.

This policy is designed to meet the requirements of the United Kingdom General Data Protection Regulation and the Data Protection Act 2018. It sits alongside our Cookie Policy, Safeguarding Policy, Complaints Policy, Equality Diversity and Inclusion Policy, and Fundraising and Donations Policy.

This policy covers the following groups. Applicants and beneficiaries. Donors, funders and prospective supporters. Trustees, staff and volunteers. Professional referrers and partner organisations. Website visitors and people who contact us by email, phone, post or web form. The policy also covers research, evaluation and case studies where relevant. The scope and structure follow charity sector practice as reflected in the example materials you provided.

Who we are and how to contact us

The Phoenix Fellowship is a registered charity in England and Wales. Our mission is to support refugee students who have overcome adversity to pursue degrees in science and medicine at British Universities and to achieve meaningful careers. We act as a data controller when we decide why and how personal data is processed.

Contact for data protection queries and rights requests. Data Protection Lead, The Phoenix Fellowship. Email: privacy@phoenixfellow.org. We aim to acknowledge rights requests promptly and respond within one calendar month in line with law and established charity practice.

The data we collect and why

Applicants and beneficiaries:

- *Identification and contact:*
    - Name, title, date of birth, contact details. We need these to administer eligibility checks, communicate decisions, and provide grants.
- *Eligibility and background:*
    - Refugee or humanitarian protection status, country of origin, education history and offers of study, financial and household information relevant to eligibility and need. This is required to assess applications fairly, to demonstrate that restricted funds are used for the intended group, and to

report impact. Comparable charities collect similar fields to assess awards and to demonstrate correct use of restricted donations.

- *Special category data where relevant and with safeguards:*
    - Health or disability information for reasonable adjustments, equality monitoring, and where pertinent to eligibility. Occasionally ethnicity and religion for monitoring and should a faith context be relevant to an award pathway. We only collect what is necessary and proportionate, apply strict access controls, and rely on an appropriate lawful basis under Article 9 as set out in section 6 below. This mirrors sector practice.
- *Safeguarding and risk:*
    - On rare occasions we may hold information relating to risk of harm or the safety of a young person or adult at risk. This information is handled under strict need-to-know access and safeguarding procedures that support statutory duties. Where appropriate we may share limited information with safeguarding authorities.
- *How collected:*
    - Directly from applicants, through our web forms or email, or by a professional referrer with the applicant's knowledge and permission.

Donors and funders

- *Contact details and communication preferences*.
    - We record name, address, email, phone, and whether you opt in to receive updates. This enables receipting, stewardship and only sending communications you have requested or would reasonably expect.
- *Donation records and Gift Aid*.
    - Amounts, dates, methods, associated declarations and relevant HMRC data so that we can process donations, comply with tax law and accounting, and analyse giving trends. Gift Aid data must be retained for audit and tax compliance.
- *Payment processing*.
    - Card and bank details are handled by secure third party payment processors and are not stored by us. We receive confirmations and non-sensitive metadata to reconcile donations and to thank donors. This approach is consistent with comparable organisations.
- *How collected*.
    - Directly from you when you donate to us or sign up for updates. Indirectly from reputable donation platforms where you have asked them to share your details with us. The example policies list such platforms and explain how data flows in stewardship contexts.

Trustees, employees and volunteers

- *Recruitment and onboarding*.

    - Application forms and CVs, references, right to work, criminal record checks where appropriate, equality monitoring, training and induction records.
- *Employment or volunteer administration*.
    - Payroll and pension administration for employees, expenses, emergency contacts, IT access, role descriptions, appraisals, and compliance training. For trustees, Companies House or Charity Commission requirements and conflict of interest registers.
- *Safeguarding checks*.
    - For roles in regulated activity or with contact with applicants, appropriate checks are undertaken through accredited providers. The examples you shared describe the use of accredited bodies and the sharing of check results on a need-to-know basis.

Website users and people who contact us

- *Analytics and site usage*.
    - We use analytics to understand visits and improve the site. This involves cookies and similar technologies that record interactions and are subject to the Cookie Policy. Example policies explain that analytics data is not used to identify individuals and is retained in line with tool default windows.
- *Web forms and enquiries*.
    - If you contact us, we collect your name and contact details and the content of your message so that we can respond to you. If you opt in to updates we will add you to our mailing list.

Children's data

We do not ordinarily accept applications from people under the age of eighteen without an adult referrer. Where an applicant is under eighteen or is a looked after child, we take additional care in how we collect, store and share their information and we may retain safeguarding records for longer to protect their vital interests, consistent with sector norms.

How we collect your data

Direct collection. Forms on our website, application portals, email and telephone, post, events and meetings. If we ask for sensitive information we explain why and ensure the request is proportionate and optional except where strictly required for eligibility or safeguarding.

Indirect collection. From a referrer such as a teacher, charity or adviser where the applicant has asked the referrer to apply on their behalf. From donation and email platforms where you have given consent to share your details with us. The examples you provided use referrers and reputable processors in similar ways.

Automated collection. When you visit our website, analytics and server logs may collect IP address, device and browser information, and pages visited as described in the Cookie Policy. Analytics retention windows commonly used by charities are referenced in the materials you shared.

Our lawful bases for using your data

- *Consent*.
    - We rely on consent for optional email updates, for processing certain special category information, for using photographs or case studies, and for sharing information with named partners in specific cases. You can withdraw consent at any time.
- *Contract*.
    - We rely on contract where it is necessary to perform or enter into an employment, consultancy or volunteering agreement, or to administer a grant with conditions.
- *Legal obligation*.
    - We process personal data to comply with law. Examples include Gift Aid, financial record keeping, prevention of fraud, and responses to lawful requests from regulators or law enforcement.
- *Legitimate interests*.
    - We process data where it is necessary for our legitimate interests and your interests and rights do not override those interests. Examples include assessing and administering grant applications, monitoring programme effectiveness, managing supporter relationships, improving our website and services, and safeguarding. The sector examples articulate similar legitimate interest uses and the related right to object.
- *Special category data and criminal offence data*.
    - Where we process special category data such as health, disability or ethnicity for fair assessment, monitoring or reasonable adjustments, we will do so under an Article 9 condition such as explicit consent or substantial public interest, and we will apply heightened safeguards. Where any criminal offence data is processed, for example in safeguarding contexts, we will do so only where permitted by law and with strict access controls, reflecting practice seen in the example policies you provided.

How we use your data

- *For applicants*.
    - To verify eligibility and need, assess applications, make award decisions, communicate outcomes, transfer funds or arrange goods and services, monitor the use and impact of awards, and evaluate and improve our programmes. We collect only what is necessary,

keep it secure and confidential, and limit access to those with a legitimate role in assessment and grant management. This use mirrors the purposes in the example grant applicant policies.

- *For donors and funders*.
    - To process and acknowledge donations, administer Gift Aid, provide updates where you have opted in, analyse giving patterns to improve stewardship, and meet accounting and audit duties. The comparable policies explain stewardship and Gift Aid obligations in similar terms.
- *For trustees, staff and volunteers*.
    - To run recruitment, safeguarding checks where appropriate, onboarding, IT access, payroll and pensions for employees, training and supervision, and to comply with employment and health and safety law. Comparable organisations describe similar uses, suppliers and access controls.
- *For website users and people who contact us*.
    - To respond to enquiries, deliver pages, maintain security and performance, and improve user experience through analytics and feedback. Example policies explain that analytics are used to improve communications and that transmission over the internet cannot be guaranteed to be completely secure.
- *Research, evaluation and case studies*.
    - We may invite applicants or alumni to share feedback or participate in surveys. Participation is voluntary and will be based on consent, with clear information about purpose, retention and publication. This approach aligns with the charity examples which describe evaluation, surveys and consent.

Sharing your data

We never sell personal data and do not allow third parties to use it for their own marketing. We share information with carefully selected service providers who act on our instructions to deliver services such as website hosting, grant or donor management systems, survey tools, secure file storage and email delivery, and payment processing. We require written contracts, confidentiality, security, restricted access, and deletion or return at the end of service.

We may share limited personal data with education partners or other charities only where it is necessary to administer a grant pathway and only with consent or another valid legal basis. Examples from the sector include sharing limited information to facilitate goods or services delivery or to consider a bursary route in principle before any identifying details are shared with consent. We may disclose information where required by law, regulation, court order or lawful request, or to protect vital interests in an emergency. In safeguarding contexts, we may share information with the police or local safeguarding teams to prevent harm, consistent

with the examples you provided.

International transfers. Some of our processors may store or access data outside the United Kingdom or the European Economic Area. Where that occurs we implement appropriate safeguards such as standard contractual clauses and risk assessments, and we ensure that your rights and effective remedies remain available. Comparable policies explain international storage for cloud and donor systems and the safeguards used.

Marketing communications

We will send email updates about our work only to people who have opted in, or where another lawful basis applies. You can unsubscribe at any time using the link in the email or by contacting us. This follows the approach in the example policies.

Cookies and analytics

Our website uses cookies for essential functionality and analytics. Analytics cookies help us understand how visitors use our site so that we can improve content and navigation. We describe cookie types, purposes, and retention in our Cookie Policy and explain how to manage preferences. Example policies describe Google Analytics usage and typical retention windows for user and event data.

Data security

We implement technical and organisational measures appropriate to the risks. These include access controls based on roles and need, encryption at rest and in transit where feasible, secure configuration and patching, multi-factor authentication for administrator access, staff and trustee training, regular reviews of processor security, and incident response procedures. Sector examples refer to physical, electronic and managerial measures, encryption where possible, locked storage for hard copy, and restricted access.

12. Data retention

We retain personal data only for as long as necessary for the purpose for which it was collected, including to satisfy legal, accounting and reporting requirements. We apply the following typical periods, subject to case specific requirements.

- *Donor and Gift Aid records*.
    - Six years from the end of the financial year of the last donation, in line with tax and audit guidance.
- *Applicants and beneficiaries*.
    - Normally six years after the end of a grant or after a final decision where no grant is awarded. Safeguarding records may be retained longer where required to protect vital interests or to meet statutory obligations. Comparable policies retain information long enough to review impact, handle queries and comply with law.
- *Trustees, employees and volunteers*.

- Six years after the end of service or employment for most records, with longer retention for pension and accident or safeguarding files where the law or risk requires this. Sector examples describe similar periods and archives.

Your rights

You have the following rights. To be informed about how we use your data. To access a copy of your personal data. To correct inaccurate or incomplete data. To request deletion in certain circumstances. To restrict or object to processing in certain circumstances including direct marketing. To data portability where applicable. To withdraw consent where consent is the basis for processing. The examples you shared list these rights and refer to the Information Commissioner's Office for guidance.

Exercising your rights. Please email or write to our Data Protection Lead with enough information to identify you and tell us what right you wish to exercise. We may ask for proof of identity where appropriate. We will respond without undue delay and within one month, unless an extension applies due to complexity, in which case we will explain why and when you can expect a full response. Guidance on preparing and submitting a subject access request is provided by the Information Commissioner's Office and is linked in the examples you shared.

Complaints. If you are unhappy with how we have handled your data, please contact us first so that we can try to resolve the matter. You also have the right to complain to the Information Commissioner's Office. Contact details and online guidance are available on the ICO website and are signposted in the example policies.

Professional referrers and partners

Where a professional referrer submits an application on an applicant's behalf, the referrer confirms they have a lawful basis to share the applicant's information with us and, where required, that they have obtained appropriate consent. We will provide privacy information to the applicant at the earliest appropriate opportunity, consistent with sector practice.

Photography, video and testimonials

We only use photographs, video or case studies with informed consent. We will explain the purpose, where they will appear, and for how long. You can withdraw consent and we will stop using the material in new publications. Where printed or shared materials already exist we will not be able to recall them, but we will not use the materials in new contexts. Example policies cover image consent within communications practice.

International supporters and processors

If you are based outside the United Kingdom, your information may be processed in the United Kingdom. Where we work with processors outside the United Kingdom or EEA, we use appropriate safeguards such as standard contractual clauses and require equivalent protections. Comparable charity policies explain use of reputable cloud and donor systems and the safeguards in place.

Contact

If you have any questions about this policy, please contact the Policy Lead using the policy@phoenixfellow.org email address.

Review

This policy is reviewed at least once a year and sooner if legal requirements or our operations change. The version number and effective date will be updated on publication.

Effective date

Effective from. 1st October 2025
Document owner. Policy Lead.
Next planned review. September 2026