

PRIVACY POLICY

Last updated: June 2026

1. PURPOSE

UKFC is committed to protecting personal data and maintaining the confidence of donors, beneficiaries, trustees, employees, volunteers, regulators, banks and stakeholders. This policy establishes the framework for lawful, fair and secure processing of personal data and supports governance, AML, sanctions compliance, fraud prevention and protection of charitable assets.

2. LEGISLATIVE AND REGULATORY FRAMEWORK

This policy aligns with UK GDPR, Data Protection Act 2018, PECR, Charity Commission guidance, Proceeds of Crime Act 2002, Terrorism Act 2000, Money Laundering Regulations 2017 (as amended), Fraud Act 2006, Bribery Act 2010, UK sanctions legislation and applicable banking expectations.

3. DEFINITIONS

Beneficial Owner

A natural person who ultimately owns, controls, or benefits from an organisation, arrangement, transaction, or asset, whether directly or indirectly. For due diligence and financial crime prevention purposes, UKFC may identify and verify beneficial owners of corporate donors, suppliers, grant recipients, partners, and other third parties where appropriate.

Consent

Any freely given, specific, informed, and unambiguous indication of a Data Subject's wishes by which they signify agreement, through a clear affirmative action, to the processing of their Personal Data.

Consent must be capable of being withdrawn at any time and shall be as easy to withdraw as it is to give.

Controller

The natural or legal person, public authority, agency, charity, or other body which, alone or jointly with others, determines the purposes and means of processing Personal Data.

For the purposes of this Policy, the UKFC acts as a Controller in relation to Personal Data it collects and processes in connection with its charitable activities, governance, fundraising, administration, and compliance obligations.

Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Data Breaches may include cyber incidents, human error, unauthorised access, accidental disclosure, loss of records, malware attacks, or other events compromising the confidentiality, integrity, or availability of Personal Data.

Data Subject

An identified or identifiable living individual to whom Personal Data relates.

A Data Subject may include, but is not limited to Trustees, Employees, Volunteers, Contractors, Donors, Beneficiaries, Grant recipients, Suppliers, Partners, Service providers, Website users or other individuals whose Personal Data is processed by UKFC.

International Transfer

The transfer, access, disclosure, storage, hosting, viewing, or processing of Personal Data outside the United Kingdom.

An International Transfer may occur where Personal Data is:

- Sent to an overseas recipient;
- Hosted on servers located outside the UK;
- Accessed remotely from another country; or
- Processed by a service provider located outside the UK.

Such transfers shall only take place where appropriate safeguards and lawful transfer mechanisms are in place.

Legitimate Interests

A lawful basis for processing Personal Data where such processing is necessary for the legitimate interests pursued by UKFC or a third party, provided those interests are not overridden by the rights, freedoms, or interests of the Data Subject.

Examples may include:

- Governance and administration;
- Fraud prevention;
- Information security;
- Risk management;
- Protection of charitable assets;
- Due diligence activities; and

- Regulatory compliance support activities.

UKFC shall conduct and document a Legitimate Interests Assessment where appropriate.

Personal Data or Personal Information

Any information relating to an identified or identifiable natural person. This includes a person's name, identification number, location data, online identifier, contact information, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

Processing

Any operation or set of operations performed on Personal Data, whether by automated means or otherwise.

Processing includes collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure, and destruction.

Processor

A natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Controller.

Examples may include cloud service providers, CRM providers, IT support providers, document storage providers, marketing service providers, and professional service providers acting under UKFC's instructions.

Processors must only process Personal Data in accordance with documented instructions from UKFC and appropriate contractual safeguards.

Sanctions Screening

The process of checking individuals, organisations, transactions, countries, vessels, or other entities against applicable sanctions lists, watchlists, and financial crime databases.

The purpose of sanctions screening is to identify and mitigate risks associated with Terrorist financing, Money laundering, Sanctions breaches, Prohibited transactions, and Reputational harm.

The UKFC will undertake sanctions screening as part of its donor due diligence, beneficiary verification, supplier due diligence, trustee due diligence, grant-making activities, and financial crime risk management processes.

Special Category Data

This is personal, sensitive data including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification purposes, and health information,

Special Category Data receives enhanced protection under UK data protection law and may only be processed where an appropriate lawful basis and additional condition for processing exists.

4. DATA PROTECTION PRINCIPLES

UKFC processes information in accordance with the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

5. GOVERNANCE AND RESPONSIBILITIES

The Board of Trustees retains ultimate accountability and oversees governance effectiveness. Management implements controls and procedures. A designated Compliance Administrator coordinates compliance. All personnel must protect information and report incidents.

6. CATEGORIES OF PERSONAL DATA

Trustee data, donor data, beneficiary data, volunteer data, employee data, contractor data, supplier data, grant information, financial information, communications records and website usage data.

7. LAWFUL BASIS MATRIX

Trustee administration – Legal obligation and legitimate interests.

Donor administration – Legitimate interests, contract and consent.

Gift Aid processing – Legal obligation.

Beneficiary assessments – Legitimate interests and substantial public interest where applicable.

Employment administration – Contract and legal obligation.

AML/KYD screening – Legal obligation and legitimate interests.

Supplier management – Contract and legitimate interests.

Marketing communications – Consent and/or Privacy and Electronic Communications Regulations (PECR) compliant legitimate interests.

8. DONOR PRIVACY PROVISIONS

UKFC shall process donor information for fundraising administration, stewardship, Gift Aid, due diligence, financial crime prevention and reporting. Donor information shall not be sold or shared for unrelated commercial purposes.

9. BENEFICIARY PRIVACY PROVISIONS

Beneficiary information shall only be collected where necessary for programme delivery, grant administration, safeguarding, monitoring and evaluation, compliance and risk management.

10. TRUSTEE PRIVACY PROVISIONS

Trustee records may include identity verification, declarations of interest, governance records, training records and due diligence documentation. Such information supports legal and governance obligations.

11. VOLUNTEER AND CONTRACTOR PRIVACY PROVISIONS

Information may be processed for recruitment, onboarding, training, supervision, safeguarding, performance management and legal compliance.

12. AML, KYD AND FINANCIAL CRIME PROCESSING

UKFC may process personal information to verify identities, assess risk, conduct sanctions screening, perform adverse media checks, investigate suspicious activity, protect charitable assets and comply with banking requirements.

13. SANCTIONS COMPLIANCE

The UKFC will screen donors, beneficiaries, trustees, suppliers, partners and grant recipients against applicable UK sanctions lists and may suspend transactions where concerns arise.

14. INFORMATION SHARING

Information may be shared with banks, auditors, accountants, professional advisers, regulators, law enforcement agencies and authorised service providers where lawful and necessary.

15. INTERNATIONAL TRANSFERS

Transfers outside the UK shall only occur where lawful transfer mechanisms and safeguards are implemented, including adequacy regulations, IDTAs or Standard Contractual Clauses.

16. INFORMATION SECURITY

Controls include access management, encryption where appropriate, MFA, secure cloud storage, password standards, endpoint protection, backups, vendor oversight, incident management and cyber-security awareness training.

17. DATA RETENTION SCHEDULE

Financial records: minimum 7 years.

Trustee records: service period plus 6 years.

Donor records: normally 7 years after last interaction.

Grant records: minimum 7 years.

Employee records: according to employment law requirements.

AML/KYD records: retained in accordance with legal and regulatory requirements.

18. INDIVIDUAL RIGHTS

Individuals may request access, correction, erasure, restriction, portability, objection and withdrawal of consent where applicable. Requests shall be handled within statutory timeframes.

19. SUBJECT ACCESS REQUEST PROCEDURE

Requests shall be logged, acknowledged, identity verified, assessed, fulfilled or lawfully refused, and retained for audit purposes. Responses shall normally be provided within one month unless an extension is permitted by law.

20. DATA BREACH MANAGEMENT

All incidents must be reported immediately. UKFC shall investigate, contain, assess, notify affected parties where required, notify the ICO where legally required and implement corrective actions.

21. TRAINING AND AWARENESS

Trustees, employees and volunteers shall receive periodic training on privacy, confidentiality, cyber security, fraud prevention, AML and sanctions compliance.

22. POLICY REVIEW

This Policy will be reviewed annually or sooner where required by changes in legislation, regulatory expectations or operational risk.

Signed by:

A handwritten signature in black ink, consisting of a large, stylized capital letter 'J' with a horizontal stroke extending to the right.

Chairman

Date: 4 June 2026