Data Protection Policy

Contents

1. Introduction 2
2. Scope 2
3. Data Controller 2
4. Disclosure 3
5. Data Collection 4
6. Data Storage 5
7. Data Access and Accuracy 6
8. Right to Erasure 6
9. Data Breach 7
10. Glossary of Terms 8
11. Appendices – Data Privacy Policy 9
    a) Privacy Statement 9
    b) How we collect personal information about you 9
    c) What information do we collect? 10
    d) Do we process sensitive personal information? 10
    e) Communications, fundraising and marketing 11
    f) Donations and other payments 11
    g) Children's data 11
    h) Other disclosures 11
    i) Security of and access to your personal data 11
    j) Your rights 12
    k) Lawful processing 13
        i. Consent 13
        ii. Contractual relationships 13
        iii. Legal obligations 14
        iv. Legitimate interests 14
        v. Achieving our mission 14
        vi. Governance 14
        vii. Publicity and income generation 14
        viii. Operational Management 14
        ix. Purely administrative purposes 15
        x. Financial Management and control 15

l) Data retention 15
m) Data storage and transmission 17
n) Policy amendments 18
o) Third party websites 18
p) Updating information 18
q) Breaches 18
r) Contact 18

1. Introduction

Endeavour collects, uses and stores certain types of information about the individuals who come into contact with the organisation in order to carry out our work. This personal data may relate to potential staff and participants, current staff and participants, former staff and participants, current and former workers, freelancers, contractors, website users, donors and contacts, collectively referred to as data subjects.

This personal information must be collected and dealt with appropriately in order to comply with the General Data Protection Regulation (GDPR).

2. Scope

This policy applies to all personal data Endeavour processes, regardless of the location where that personal data is stored and regardless of the data subject. All staff and volunteers processing personal data on Endeavour's behalf must read it. A failure to comply with this policy may result in disciplinary action. Endeavour Staff includes employees, casual workers, sessional staff, freelancers and anyone else receiving payment for work at Endeavour.

3. Data Controller

Endeavour is registered as a Data Controller under GDPR, which means that it determines what purposes personal information is held and how it will be used. It is also responsible for notifying the Information Commissioner about the data it holds or is likely to hold, and the general purposes that this data will be used for.

Due to the nature of the data controlled and processed by Endeavour, we are not required to appoint a Data Protection Officer, however, Endeavour's designated Data Controller is the Chief Executive Officer.

4. Disclosure

Endeavour may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The individual will be made aware in most circumstances how and with whom their information will be shared. There are however some circumstances where the law allows Endeavour to disclose data (including special category data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State
b) Protecting vital interests of individuals e.g. safeguarding
c) Where the individual has already made the information public
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
e) Monitoring for equal opportunities purposes – e.g. race, disability or religion
f) Providing a confidential service where the individual's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where it is in the best interest of the individual

Endeavour regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Endeavour intends to ensure that personal information is treated lawfully and correctly. To this end, Endeavour will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulation.

Specifically, the Principles require that personal information is:

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 purposes or statistical purposes shall not be considered to be incompatible with the initial purpose;
3) Accurate and, when necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
4) Kept in a form that 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 processes 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

measured required by GDPR in order to safeguard the rights and freedoms of individuals;

5) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Endeavour will, through appropriate management and strict application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under GDPR. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

5. Data Collection

Endeavour will ensure there is a valid lawful basis in order to process personal data. The six lawful bases for processing data under GDPR are:

1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose
2) Contract: the processing is necessary for a contract you have with an individual, or because they have asked you to take specific steps before entering the contract
3) Legal obligations: the processing is necessary for you to comply with the law (not including contractual obligations)

4) Vital interest: the processing is necessary to protect someone's life
5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
6) Legitimate interest: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

When processing data under the 'consent' legal basis, Endeavour will always work to seek informed consent. Informed consent is when:

- An individual clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent

Endeavour will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

In accordance with the GDPR guidelines, Endeavour considers children aged 13 to 18 able to consent to legitimate communications from the organisation. When personal or sensitive information needs to be collected or shared, we will also seek to gain consent from a parent or guardian in line with good practice guidelines.

When collecting data, Endeavour will ensure that the individual:

a) Clearly understands why the information is needed and how it will be used
b) Understands what it will be used for and what the consequences are should the individual decide not to give consent to processing
c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

6. Data Storage

Information and records relating to individuals will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed and will be disposed of appropriately and confidentially.

It is Endeavour's responsibility to ensure all personal and company data is non-recoverable from any data storage previously used within the organisation, which has been passed on/sold to a third party.

7. Data Access and Accuracy

All individuals have the right to access the information Endeavour holds about them. Endeavour will also take reasonable steps to ensure that this information is kept up to date by asking current data subjects whether there have been any changes.

In addition, Endeavour will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection. The individual responsible is the Chief Executive Officer
- Everyone processing personal information understands that they are responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will review and conduct internal audits of the ways it holds, manages and uses personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

All requests for information relating to data should be forwarded to the Chief Executive Officer who will deal with the request in line with this policy.

This policy will be reviewed and updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations or Endeavour's Capability, Disciplinary and Grievance Policy.

8. Right to Erasure

Endeavour will comply with Article 17 of the GDPR which states that individuals have the right to have personal data erased in certain circumstance. The 'right to be forgotten' applies if:

- The personal data is no longer necessary for the purpose which Endeavour originally collected or processed it for;
- Endeavour is relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

- Endeavour is relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- Endeavour is processing data for direct marketing and the individual objects to that processing;
- Endeavour has processed the data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- Endeavour has to do it to comply with a legal obligation; or
- Endeavour has processed the personal data to offer information society services to a child

The 'right to be forgotten' does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom or right of freedom and expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing;
- For the establishment, exercise or defence of legal claims

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices)
- If the processing is necessary for the purposes of preventative or occupation medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data being processed is being processed by or under the responsibility of a professional subject to legal obligation of professional secrecy (e.g. as a health professional)

Endeavour will seek to act upon all legitimate 'right to be forgotten' requests within one month of receipt of the request.

9. Data Breach

If a suspected data breach occurs, the Chief Executive Officer, Director of Finance and Resources and a Board Member will meet as soon as possible in order to gather all relevant information to determine:

- Whether or not a breach has occurred

- Exactly what information may have been compromised
- The sensitivity of the information
- Whether or not there is a high risk of adversely affecting the individuals involved
- If the individuals involved need to be notified

If it is determined that a data breach has occurred, the incident will be reported to the ICO within 72 hours of becoming known to Endeavour.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Endeavour will inform the individuals without undue delay.

A record of all breaches will be maintained.

10. Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information Endeavour will hold and how it will be held or used.

General Data Protection Regulations – The framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Endeavour follows its data protection policy and complies with the General Data Protection Regulations.

Individual – The person whose personal information is being held or processed by Endeavour for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Participant in the processing of personal information about them. Explicit consent is needed for processing special category data.

Notification – Notifying the Information Commissioner about the data processing activities of Endeavour, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the General Data Protection Regulation.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Endeavour.

Special category data – refers to data about:

- Racial or ethnic origin

- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

11. Appendices – Data Privacy Policy

a) Privacy Statement

We are committed to safeguarding your privacy. At all times we aim to respect any personal data you share with us, or that we receive from other organisations, and keep it safe. This Privacy Policy sets out our data collection and processing practices and your options regarding the ways in which your personal information is used.

Should you need to contact anyone at Endeavour regarding this policy please address your query to the DPO (Data Processing Officer) at:

Email: info@endeavour.org.uk

Phone: 0114 243 8219

This Policy contains important information about your personal rights to privacy. Please read it carefully to understand how we use your personal data.

The provision of your personal data to us is voluntary. However providing us with your personal data means you will be able to, participate in our programmes, access our training, attend our meetings, make a donation, apply for employment, volunteering or other work with us and allow us to promote our offers and case studies more widely.

b) How we collect personal information about you

We may ask to collect personal information from you when you interact with Endeavour. There are lots of different examples of interaction which include: If you enquire about our work, or our events, if you make a donation, or apply for a job or volunteer with us or provide us with personal information if you participate in one of our projects or programmes. This may be when you phone us, email us, visit our website, and sign up to attend an event or training session, through the post or in person.

We will ask for personal information DIRECTLY if you wish:

- To access specialist support
- To attend our training
- To attend meetings or events
- When you apply for employment, volunteering of other work
- When you purchase services from us

- When you register for any of the programmes we deliver

c) What information do we collect?

We may collect, store and use the following kinds of personal data:

- Your name and contact details
- Next of Kin or Emergency contact details
- Medical information
- Further information such as support needs for a disability or Faith requirement
- Consent to participate
- Consent to utilise photo or video images
- Postal address
- Telephone number
- E-mail address
- Any other information you have chosen to share with us

However, we may request other information where it is appropriate and relevant, for example

- Details of why you have decided to contact us and notes relating to any discussions in person or electronically
- Your bank details or debit/credit card details for processing payments;
- Photographic images of your likeness
- Details of your interests and participation in our work, surveys you have completed, etc

d) Do we process sensitive personal information?

Applicable law recognises certain categories of personal information as sensitive and therefore require more protection including information for equal opportunities monitoring (where appropriate). We may also collect and store sensitive personal data if there is a clear reason for doing so; and will only do so with your explicit consent or where the law requires us to do this.

How and why will we use your personal data?

Personal data, however it has been provided to us, will be used for the purposes specified in this Policy or in relevant parts of the website.

We may use your personal information to:

- Enable you to use any and/or all of the services we offer;
- Send you information about our work, campaigns, programmes and any other information, products or services that we provide. The channels we will use to do this are: phone, email, direct mail and digital advertisements (this will not be done without your consent and you may specify which channels of communication you prefer);
- Provide you with the services, products, programmes or information you have requested;

- Handle the administration of any donation or other payment you make via credit/debit card, cheque, standing order or BACS transfer;
- Collect payments from you and send statements and/or receipts to you;
- Handle the administration of your employment, volunteering or any other work you apply for and are engaged on;
- Conduct research into the impact of our events;
- Deal with enquiries and complaints made by or about you
- Make applications for accreditation by third parties, where you have registered
- Audit and/or administer our accounts.

e) Communications, fundraising and marketing

Where you have provided us with your physical address, we will contact you by post; and where you have provided appropriate consent, also by telephone and e-mail, with targeted communications to let you know about our work, events, campaigns and other activities that we consider may be of particular interest; about the work of Endeavour and to ask for donations or other support.

f) Donations and other payments

All financial transactions carried out on our website are handled through Just Giving and Stripe, third party payment services providers. We recommend that you read their privacy policies (available at https://www.justgiving.com/about/info/privacy-policy/privacy-policy-v30 and https://stripe.com/gb/privacy) prior to effecting any transactions with us.

We will provide your personal data to these organisations only to the extent necessary for the purposes of processing payments for transactions you enter into with us. We reserve the right to change our third party payment service providers subject to the needs of our business, without need for notice, this Privacy Policy should therefore be checked regularly for updates. We do not store your financial details for any of these web based payments.

g) Children's data

We may process data of people under the age of 18 that participate in our programmes. Where we do this information will be encrypted and access to this information limited to those staff requiring it in order to run the programme and provide necessary reporting only to our funders. We will securely store this information for a reasonable period and as required by company, funder or for legal reasons.

h) Other disclosures

We will disclose your information to regulatory and/or government bodies and/or law enforcement agencies upon request only when required to do so in order to satisfy legal obligations which are binding on us.

i) Security of and access to your personal data

We take the security of your personal information extremely seriously. We've implemented appropriate physical, technical and organisational measures to

protect the personal information we have under our control, both on and offline, from improper access, use, alteration, destruction and loss.

Your information is only accessible by appropriately trained staff, volunteers and contractors, or contracted agencies and/or suppliers who are processing data on our behalf.

Otherwise than as set out in this Privacy Policy, we will only ever share your data with your informed consent.

j) Your rights

Where we rely on your consent to use your personal information, you have the right to withdraw that consent at any time. This includes the right to ask us to stop using your personal information for direct marketing purposes or to be unsubscribed from our email list at any time. You also have the following rights:

- Right to be informed
    - You have the right to be told how your personal information will be used. This Policy and other policies and statements used on our website and in our communications are intended to provide you with a clear and transparent description of how your personal information may be used.
- Right of access
    - You can write to us to ask for confirmation of what information we hold on you and to request a copy of that information. Provided we are satisfied that you are entitled to see the information requested and we have successfully confirmed your identity, we have 40 days to comply. As from 25 May 2018, we will have 30 days to comply.
- Right of erasure
    - As from 25 May 2018, you can ask us for your personal information to be deleted from our records. In many cases we would propose to suppress further communications with you, rather than delete it so that we have evidence of your request for audit purposes.
- Right of rectification
    - If you believe our records of your personal information are inaccurate, you have the right to ask for those records to be updated.
- Right to restrict processing
    - You have the right to ask for processing of your personal data to be restricted if there is disagreement about its accuracy or legitimate usage.
- Right to data portability
    - to the extent required by the General Data Protection Regulations ("GDPR") where we are processing your personal information under your consent, because such processing is necessary for the performance of a contract to which you are party, to take steps at your request prior to entering into a contact or by automated means,

you may ask us to provide this information to you – or another service provider – in a machine-readable format.

To exercise these rights, please send a description of the personal information in question using the contact details below.

We also have specific pages to unsubscribe from our email list which can be found in the footer of all our marketing emails.

Where we consider that the information with which you have provided us does not enable us to identify the personal information in question, we reserve the right to ask for personal identification and/or further information.

Please note that some of these rights only apply in limited circumstances. For more information, we suggest that you consult ICO guidance – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ – or please contact us using the details below.

You are further entitled to make a complaint about us or the way we have processed your data to the Information Commissioner's Office ("ICO"). For further information on how to exercise this right, please see the guidance at https://ico.org.uk/for-the-public/personal-information. The contact details of the ICO can be found here: https://ico.org.uk/global/contact-us/.

k) Lawful processing

We are required to have one or more lawful grounds to process your personal information. Only 4 of these are relevant to us:

1. Personal information is processed on the basis of a **person's consent**
2. Personal information is processed on the basis of a **contractual relationship**
3. Personal information is processed on the basis of **legal obligations**
4. Personal information is processed on the basis of **legitimate interests**

i. Consent

We will ask for your consent to use your information to contact you by phone, send you electronic or postal communications such as newsletters and marketing and fundraising emails, for targeted advertising and profiling, and if you ever share sensitive personal information with us. Where our programmes are enhanced by the sharing of information (i.e. Local partnerships or training) we will ask your consent to share with other relevant parties.

ii. Contractual relationships

Many of our interactions with users are voluntary and not contractual. However, sometimes it will be necessary to process personal information so

that we can enter contractual relationships with people. For example, if you apply for employment or to volunteer with us, if you book on our events, participate in programmes or purchase something from us.

iii. Legal obligations

Sometimes we will be obliged to process your personal information due to legal obligations which are binding on us. We will only ever do so when strictly necessary.

iv. Legitimate interests

Applicable law allows personal information to be collected and used if it is reasonably necessary for our legitimate activities (as long as its use is fair, balanced and does not unduly impact individuals' rights).

We will rely on this ground to process your personal data when it is not practical or appropriate to ask for consent.

v. Achieving our mission

- This includes (but not limited to) To assist young people to develop their full potential as individuals and as members of society.

vi. Governance

- Internal and external audit for financial or regulatory compliance purposes
- Statutory reporting

vii. Publicity and income generation

- Conventional direct marketing and other forms of marketing, publicity or advertisement
- Unsolicited commercial or non-commercial messages, including campaigns, newsletters, income generation or charitable fundraising
- Analysis, targeting and segmentation to develop and promote or strategy and improve communication efficiency
- Dissemination of our work through our website, publications, conferences, training events and social media
- Personalisation used to tailor and enhance your experience of our communications

viii. Operational Management

- Employee, contractor and volunteer recording and monitoring for recruitment, safety, performance management or workforce planning purposes
- Provision and administration of staff benefits such as pensions
- Physical security, IT and network security

- Maintenance of suppression files
- Processing for historical, scientific or statistical purpose

ix. Purely administrative purposes

- Responding to enquiries
- Delivery of requested products or information
- Communications designed to administer existing services including administration of programmes and financial transactions
- Thank you communications and receipts
- Maintaining a supporter database and suppression lists

x. Financial Management and control

- Processing financial transactions and maintaining financial controls
- Prevention of fraud, misuse of services, or money laundering
- Enforcement of legal claims
- Reporting criminal acts and compliance with law enforcement agencies

When we use your personal information, we will consider if it is fair and balanced to do so and if it is within your reasonable expectations. We will balance your rights and our legitimate interests to ensure that we use your personal information legally and fairly.

l) Data retention

In general, unless still required in connection with the purpose(s) for which it was collected and/or is processed as outlined in our Data Retention Schedule, we remove your personal information from our records. However, if before that date your personal information is no longer required in connection with such purpose(s), we are no longer lawfully entitled to process it or you validly exercise your right of erasure, we will remove it from our records at the relevant time.

The below list is an example of some of our specific retention periods, please note this list is not exhaustive and is determined by the purpose we collected your data.

Record	Retention period
Accident books, accident records, accident reports	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches age 21).
Accounting records	Six years

Record	Retention period
Application forms and interview notes (for unsuccessful candidates)	Six months.
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently.
Control of Substances Hazardous to Health Regulations (COSHH) records of tests and examinations of control systems and protective equipment	Five years from the date on which the tests were carried out.
DBS certificate information	Three years or until superseded if less.
Driving licence, vehicle insurance, MOT certificate details	One year after expiry unless renewed.
Expatriate records and other records relating to foreign employees (e.g. visa, work permits, etc.)	Six years after employment ceases.
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than three years after the end of the financial year to which they relate.
Parental leave records	Five years from birth/adoption of the child or 18 years if the child receives a disability living allowance. *Recommended.*
Personnel files and training records (including disciplinary records and working time records)	Six years after employment ceases.
Records relating to children and young adults	Until the child/young adult reaches age 21.

Record	Retention period
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	Six years from the date of redundancy.
SMP, SAP, SSPP records, calculations, certificates (Mat B1s) or other medical evidence, notifications, declarations and notices	Three years after the end of the tax year in which the leave period ends.
Statutory Sick Pay records, calculations, certificates, self-certificates	Six years after the employment ceases.
Trust deeds and rules	Permanently.
Trustees' minute books	Permanently.
Wage/salary records	Six years.

In the event that you ask us to stop sending you direct marketing / fundraising / other electronic communications, we will keep your name on our internal suppression list to ensure that you are not contacted again.

m) Data storage and transmission

How information is stored:

- Physical personal information is kept in non-portable locked cabinets with access limited to those who need to see it eg staff employment & payroll records accessed by senior management and HR/finance staff, young people's consent forms accessed by operational staff.
- Electronic data is stored at the following Microsoft datacentres:
    - Exchange Online - United Kingdom
    - Exchange Online Protection - European Union
    - Microsoft Teams – United Kingdom
    - OneDrive - United Kingdom
    - SharePoint - United Kingdom
    - Viva Connections – European Union

- Electronic data on SharePoint is stored and encrypted with one or more AES 256-bit keys. Sensitive data (eg payroll records) is also saved in password protected documents.

- Email is encrypted:

    - At rest – Bitlocker
    - In transit – DKIM and TLS

n) Policy amendments

We keep this Privacy Policy under regular review and reserve the right to update from time-to-time by posting an updated version on our website, not least because of changes in applicable law.

We recommend that you check this Privacy Policy occasionally to ensure you remain happy with it. We may also notify you of any important changes to our privacy policy by email.

This Privacy Policy was last updated on 19 March 2025.

o) Third party websites

We link our website directly to other sites. This Privacy Policy **does not** cover external websites and **we are not responsible** for the privacy practices or content of those sites. We encourage you to read the privacy policies of any external websites you visit via links on our website. Updating your information on third party websites will not be shared with us unless you give consent or there is a legal or contractual reason for processing.

p) Updating information

You may ask us at any time to update your details, correct or remove information you think is inaccurate or to check the information we hold about you by contacting us via post or email.

q) Breaches

All data breaches will be assessed using the Information Commissioners Office (ICO) Self-Assessment tool to determine whether the breach needs to be reported to the ICO.

You will be notified of any breach, the nature of this, what has happened, the likely consequences and any action being taken by us. You will also be provided with contact details of the person to refer to for more information.

r) Contact

We are registered with the Information Commissioners Office (ICO). The Chief Executive is our Data Processing Officer. Please let us know if you have any queries or concerns whatsoever about the way in which your data is being processed by either emailing us at info@endeavour.org.uk, telephone 0114 243 8219 or writing to us at Endeavour Centre, Earl Marshal Road, Sheffield, S4 8FB.