Data Protection Policy

Introduction

Data Protection law places obligations on Demographic User Group with regard to the collection, use and storage of personal information. The UK's data protection regulator, the Information Commissioner's Office (ICO), has powers to impose substantial fines and other sanctions for failure to comply with our obligations and for actual data breaches.

Certain pieces of legislation set out types of information and data that we are legally required to keep and for how long we should keep them. They also require that we do not retain data and information about our supporters, staff, or other people who can be identified where there is no reasonable business need.

Policy

Demographic User Group is committed to ensuring the confidentiality, integrity and availability of personal information:

- Confidentiality means ensuring that personal and confidential information is not disclosed, either purposefully or accidentally, to people who do not have the right to see it.
- Integrity means ensuring that data is accurate and up to date.
- Availability means ensuring that data is available to those who are authorised to see it.

Demographic User Group exercises the responsible stewardship of personal data as part of its vision to make the UK home to the most ambitious firms in the World. Information plays an important role in enabling Demographic User Group to do its work. We are committed to the organised, confidential and secure collection, creation, retrieval, storage, handling, transfer and preservation of this information; and to identifying and securely destroying information where it has no continuing business, legal or historical significance.

Scope of this Policy

This Policy covers the collection, use, storage or transfer of any 'personal data' (including 'sensitive personal data') and other forms of data and information by Demographic User Group, or by anyone processing data on our behalf.

'Personal data' is any information that relates to an identifiable living individual that is stored electronically or in a searchable paper filing system. Examples may include:

- Names and contact details (eg phone, email, address);
- Financial information (eg credit card, donation amounts);
- Any other personal details (eg family circumstances, medical history and, in some circumstances, photographs of people).

'Sensitive personal data' is data about an individual's racial or ethnic origin, religious or other beliefs, criminal record, sexual life, trade union membership, medical information or political opinions. The law places additional requirements on processing sensitive personal data.

This Policy applies to personal data in all its forms: whether on paper, stored electronically, held on film, microfiche or other media. It includes pictures, video and audio as well as text. It covers information transmitted by post, electronically, and by oral communication (including telephone and voicemail). It applies throughout the lifecycle of the information and data from its creation/collection through its use and storage to its disposal.

This policy applies to Demographic User Group's Directors, staff, advisers, assessors, ambassadors and contractors. With regard to electronic systems it applies to the use of Demographic User Group's own computer network and databases and externally or privately-owned systems when connected to Demographic User Group network.

Policy Framework

This Policy should be read alongside the other policies that form our approach to the proper use, management, security and destruction of data and information. The other policies in the data and information policy frameworks are:

- IT Acceptable Use Policy
- Confidentiality Policy
- Records Management Policy
- Information Security Policy

Collecting, Handling & Processing Data and Information

In collecting, handling and processing personal data, Demographic User Group will:

- Be open and honest with individuals whose information we hold; and
- Respect Individuals' rights.

When we collect personal data, we will do so fairly, lawfully and in line with specified purposes and we will not keep data for longer than necessary. Demographic User Group operates under the following legal bases:

- **Consent** – for marketing emails and to process sensitive information about staff. This means we offer individuals a real choice and control over their data and require a positive opt-in.
- **Legitimate interest** – for processing the data of the users of our programmes.
- **Contract, legal obligations and legitimate Interests** – for dealing with job applicants, employees, volunteers and trustees. This means we use the contractual legal basis when we need to fulfil our contractual obligations.

When we store and use personal data we recognise that our main priority is to avoid causing harm or distress to individuals. Data must be kept securely and be as accurate as possible. Staff members must only view, process, access or disclose personal data if they "need to know" the information for the purpose of providing Be the Business's services, or the day to day operation of the charity. Access to personal data must be limited to the minimum amount of personal data necessary for the purpose. We must make sure that data is kept up-to-date and take reasonable precautions against inadvertent or inappropriate disclosure or access.

Data must not be sent outside of the European Economic Area without special arrangements in place (speak to DPO if this is proposed).

If individuals whose data we process exercise their legal right to make a request about their data, we must respond promptly and in line with the law. This means that our personnel, and anyone working on our behalf, must:

- Understand and maintain clear accountability for data protection;
- Understand our responsibilities when managing and handling data and are therefore appropriately trained and supervised;
- Follow procedures for collecting, storing and using data;
- Promptly and courteously deal with queries about data.

Regular reviews are made of the way we collect, store and use data.

Data and Information Classifications

We classify data and the information that we keep in the following ways:

Table One

Classification	Definition	Examples
Sensitive	Information for which unauthorised disclosure (internally or externally) may cause serious financial or reputational damage, or legal action. Note: some information may only be considered 'Sensitive' for a short period of time.	Sensitive medical information or employment information about staff, Trustees or Committee members Al information relating to Mentors and Mentees
Confidential	Intended for distribution within the organisation whether to just one, some, or all colleagues. We would not want or need to publicise the information.	Bank Statements Staff or supporters' contact details Google Analytics data Policies and standards Process documents Internal announcements Staff handbook
Unrestricted	Intended for the public so zero impact if the information is made public.	Marketing materials Job advertisements Public announcements Publicly-accessible website Internally generated Social media content

Data Incidents

We have a data breach procedure which governs our approach to managing and reporting breaches. If the breach is notifiable, we will contact the ICO within the required 72-hour reporting period.

A data incident is "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 Subject Access Requests

We have a Subject Access Request (SAR) procedure which governs our approach to managing requests by individuals to their personal data held by Demographic User Group. Request can be made verbally or in writing and in most cases must be handled within 30 days. Demographic User Group Data Protection Officer is responsible for managing the SAR process.

Disclosures

There is a legal duty to disclose some information including:

- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.
- In addition, a colleague believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the CFO who will report it to the appropriate authorities.

Demographic User Group complies fully with the CRB Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it. Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept. However, Demographic User Group may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Sharing Data & Information

We often need to share data with third parties for various essential business processes – e.g, for analytics software, email marketing, processing data for campaigns, CRM and administration of our employee payroll.
Even though we may use service providers and partners who collect, store or use personal data on our behalf, we remain responsible for that data in almost all cases. Therefore, we must ensure that those service providers have suitable systems, procedures and staff in place, have a written contract with us and, in some cases, a Non-Disclosure Agreement (NDA).

Before you transfer any data, ensure that:

- The transfer is really necessary. Do not move data unless you really need to.
- Don't transfer more than is needed. Reduce the amount of data you move to reduce the risk and consequential damage if it does get lost. Consider sending only those records that are needed or only the specific fields that are required.
- Make certain that the recipient of the data is authorised to receive and process it.

- Make certain that the recipient of the data has adequate security measures (which can include encryption or pseudonymisation) to safeguard the data.

Methods of transfer

Having established that a transfer is required and reduced the data to the minimum necessary, it's important to consider HOW the data will be transferred.

Transferring personal identifiable information data via email is not desirable and should be avoided wherever possible. The main problem with email is that, in most cases, the message is not transmitted directly from sender to receiver – there may be several server-to-server hops for the message, each one of which is a potential resting place for a copy of the original message.

Additionally, a copy of the data sent is likely to remain in the accounts of both sender and recipient and on the email servers of the respective locations.

If this kind of transfer is unavoidable then the following guidelines should be undertaken:

- Ensure that the data is minimised and de-personalised where possible.
- Protect the data with strong encryption before attachment.
- Send strong, unique passwords to your recipient separately – preferably by telephone rather than another email message.
- Ask for a tracking receipt so you know when the email is opened.
- Delete the attachments/sent email, plus and draft copies, after the message receipt is confirmed

Physical transfer by courier or post

Physical media (eg USB or disc etc) transfer carries a much higher risk of data getting lost, damaged or delivered to the wrong person. If this is the only method of data transfer available then the following guidelines should be followed:

- Ensure that your data is minimised – and preferably depersonalised.
- Protect the data with strong encryption, where possible
- Send strong, unique passwords to your recipient by a separate means.
- Use a courier with a specialist data service if possible.
- Confirm delivery with your recipient.
- Ensure that signatures and receipts are readable and available quickly.

Retaining Data & Information

Demographic User Group retains information and data for three key reasons:

- To comply with legislation and established best practice;
- To support our day to day activities and inform our longer-term planning;
- To tell the essential 'story' of Demographic User Group and its activities over time.

Demographic User Group Retention Schedule sets out the periods that different types of data and information should be held for and also provides the data classification which will inform how data is transferred and ultimately disposed of.

Personal Identifiable Information should not be held longer that stated in the Retention Schedule otherwise we will be failing in our responsibilities under the General Data Protection Regulation.

Disposing of Data & Information

At the end of an agreed retention period, data and information will be securely and confidentially destroyed, subject to its classification. Examples of classifications are provided in Table On and more detailed information is available in the Retention Schedule.

Secret and Confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure. Confidential and Secret information on paper should be shredded. Unwanted paper documents that do not contain any Secret or Confidential information should be disposed of by recycling.

For the disposal of electronic equipment, please see the Information Security Policy

Process and authority for destruction of data:

On an annual basis the Data Protection Officer will issue instructions and a schedule to the relevant internal stakeholders for the systematic disposal of data in accordance with our Retention Schedule. The Data Protection Officer may also issue notices for the removal, deletion and disposal of data and information on an ad hoc basis when necessary.

Associated Legislation, Guidance, References and Documents

Data Protection Legislation sets out essential principles, which are the foundation on which our organisation is bound and measured.

The **General Data Protection Regulation** (GDPR) is a Europe-wide law that replaces the Data Protection Act 1998 in the UK.

The **Data Protection Act 2018** is the UK's implementation of the derogations of the GDPR. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'.

PECR are the Privacy and Electronic Communications Regulations. Their full title is The Privacy and Electronic Communications (EC Directive) Regulations 2003.

They are derived from European law. They implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.

Prepared by:	Jan Wright 7th February 2021
Approved by:	
Date Approved:	
Review date:	