Data Protection Policy

Statement of Policy

Humanimal Trust needs to gather and use certain information about individuals for a variety of purposes. The data gathered will relate to supporters, employees, volunteers, suppliers and any other people or organisations that the Trust has a relationship with or may need to contact.

This policy sets out Humanimal Trusts commitment to protecting personal data and ensuring that all staff and volunteers, where relevant, understands the rules governing the use of personal data which they have access to during the course of their work or volunteering activity.

Purpose

The principles underlying this data protection policy ensures that Humanimal Trust:

- Complies with Data Protection Legislation and follows good practice
- Protects the rights of staff, volunteers, supporters and partners
- Is open about how we store and process individuals' information
- Protect ourselves from the risk of data breach or attack on any of our systems.

Definitions

The purposes for which personal data may be used by us:

- HR
- Administrative
- Financial
- Regulatory
- Payroll
- Charity Development

Charity Development includes the following:

- Compliance with our legal, regulatory and charity governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring charity policies are adhered to I.e., policies covering email and internet use.
- Operational reasons such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting, credit scoring checking.
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff absences, administration and assessments.
- Monitoring staff and volunteer conduct, disciplinary matters

- Charity marketing and fundraising activity
- Improving our services

Personal Data

- Information relating to identifiable individuals such as job applicants, current and former employees, volunteer applicants, volunteers, trustees, agency, contract and other staff, supporters, suppliers and marketing contacts.
- Personal data we gather may include individuals contact details, educational background, pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.

Sensitive Personal Information

- Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings.
- Any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all staff and volunteers who must be familiar with and fully comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy with additional policies or guidelines from time to time. Any new or modified policies will be circulated to all staff/volunteers prior to being adopted.

As our Data Protection Officer (DPO), the CEO has overall responsibility for the day-to-day implementation of this policy. The Trusts' Chair and Trustees (Board of Trustees) retains overall responsibility for compliance with the new UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 which has been amended to be read in conjunction with it.

Our Procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. You must record this consent or non-consent where personal data is stored in CRM.

The Data Protection Officer (DPO) is Responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders.
- Responding to individuals such as supporters and employees who wish to know which data is being held on them by Humanimal Trust.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from supporters, target audiences or media outlets
- Coordinate with the IT Support Service/DPO to ensure that all marketing initiatives adhere to data protection laws and Humanimal Trusts Data Protection Policy

Responsibilities of the IT Support Service/DPO

- Ensure all systems, services, software, updates and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

The Processing of all Data must be:

- Necessary to deliver our services.
- In our legitimate interests and must not unduly prejudice the individual's privacy.
- In most cases this provision will apply to routine charity data processing activities.

Our website contains our **Privacy Statement** to supporters with regards data protection.

The Privacy Statement:

- Sets out the reasons why we hold personal data for supporters, volunteers, suppliers and employees.
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers.
- States that supporters and others have a right of access to the personal data that we hold about them.

Sensitive Personal Data

In most cases where we process sensitive personal data, we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g., to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

We will ensure that any personal data that we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any other unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If they believe that the information that we hold is inaccurate then this fact should be recorded and that the accuracy of the information we hold is disputed and inform the DPO.

Your Personal Data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data Security

You must ensure that you keep all personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases where data is stored on printed paper, it should be kept in a secure location where it cannot be accessed by any unauthorised personnel.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords. All passwords must be encrypted (cannot be read in plain text).
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The DPO must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up.
- Where possible, data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- Any servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention

We must not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into consideration the reasons that the personal data was obtained,

but should be determined in a manner consistent with our data retention guidelines. Please refer to Humanimal Trusts Data Retention Schedule for recommended retention periods

Transferring data internationally

There are strict restrictions on international transfers of personal data. Personal data must not be transferred anywhere outside the UK without first consulting the Data Protection Officer. The DPO must ensure that the country or organisation in question can guarantee an adequate level of protection for the processing of personal data. If personal data is transferred electronically, via email or web services, all these services must be secure and use approved encryption methods. Specific consent must be obtained from the data subject before sending any of their data outside the UK.

Subject Access Requests

Under the UK General Data Protection Regulations (GDPR), individuals are entitled, subject to certain exceptions, to request access to information held about them either verbally or in writing.

Where we are in receipt of a subject access request, this should be referred, immediately, to the DPO. We may ask for some additional information to enable us to comply with that request. Such a request must be responded to promptly at the very latest, within one month of receiving the request. We are able to extend this request by a further two months if the request is complex or we are in receipt of a number of requests from the individual relating to individual rights.

The Data Protection Officer should be contacted if individuals would like to correct any information that we hold about them. There are also restrictions on the information to which they are entitled under applicable law.

Processing Data in accordance with the Individual's Rights

You must abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request. This should be recorded where the personal data is stored.

We will not send direct marketing material to someone electronically (e.g., via email) unless we have an existing relationship with them in relation to the charity.

The DPO must be referred to for advice on direct marketing before undertaking any new direct marketing activity.

Training

All staff and volunteers will receive training on this policy and new joiners will receive training as part of the induction process. Further training will be provided annually or whenever there is a substantial change in the law or our policy and procedure.

Training is provided by via HR Provider, Atlas – Citation on a regular basis.

This training will cover:

- The law relating to data protection.
- Our data protection and related policies and procedures.

Completion of this training is compulsory.

Privacy Notice - Transparency of Data Protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	Humanimal Trust
How is it collected?	Online, by phone, email
Why is it being collected?	See definitions section above
How will it be used?	See definitions section above
Who will it be shared with?	No-one unless we have explicit consent
Identity and contact details of any data controllers	Trust's Chair and Trustees (The Board)
Retention period	Please refer to Humanimal Trusts Retention Schedule for full details

Conditions for Processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for Personal Data

We will process personal data in compliance with all data protection principles as detailed in UK GDPR and the Data Protection Act 2018.

We will document any additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject has the right to receive a copy of their data in a structured format. These requests should be processed within one month of receipt, provided there is no undue burden, and it does not compromise the privacy of any other individuals. A data subject may also request that their data is transferred directly to another system and must be carried out free of charge,

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. This includes removal of data from data back- ups, if back-ups are done regularly this should suffice.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting Breaches

All members of staff and volunteers have an obligation to report actual or potential data protection compliance failures to the DPO immediately. This allows us to:

- Investigate any failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material in their own right, or as part of a pattern of failures. Under the GDPR (General Data Protection Regulation), organisations must report certain types of data breach to their supervisory authority within 72 hours of becoming aware of it.

See link below:
https://www.itgovernance.eu/blog/en/how-to-report-a-data-breach-to-your-supervisory-authority

Monitoring

Everyone must observe and adhere to this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

Consequences of Failing to Comply

We take compliance with this policy very seriously. Failure to comply puts both the individual and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything detailed in this policy, do not hesitate to contact the DPO.

Updated 19th January 2024