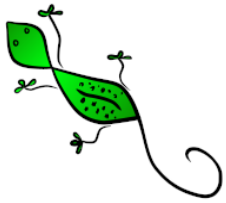
Data Protection and GDPR Policy



Gecko Community

Empower, Inspire, Educate

Contents:

A Short Guide to Data Protection and You

1. What is Data Protection?

Data protection is a series of laws, processes and policies that ensure organisations and individuals safeguard any and all personal data they hold and process.

Data protection laws only relate to data about a living individual. The Data Protection Act covers 4 types of data;

1. Information processed, or intended to be processed by automatic means.
    a. Generally, this is computer held data.
2. Information processed in a non-automated manner, which forms part of, or is intended to form part of a 'filing system'.
    a. Generally, this is a paper filling system.
3. Information that forms part of an 'accessible record'
    a. This is information such as health records etc. parts of which may be accessed by different organisations.
4. Information held by a public authority
    a. This type of information is referred to as category E data.

2. What data is covered under Data Protection?

Data protection laws split our data between two main categories;

- Personal Data
- Special Category information

Personal data means any information relating to an identified or identifiable natural person (Data Subject).

The identifiable categories are:

- Name
- Unique Learner Number
- Online Identifier
- Photos
- Description
- Address
- Email Address
- Telephone Numbers

Special Category data covers more sensitive data, such as:

- Race
- Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Genetic Data
- Health and Medical Data

3. What about GDPR?

GDPR or General Data Protection Regulation, is an additional set of laws, processes and procedures, that came into effect in May 2018. GDPR advances and updates the Data Protection law, it does not replace it.

GDPR focuses more on the protection of the data subjects and clears up any grey areas surrounding the use of digital media.

The eight main focuses and rights of GDPR are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right of data portability
7. The right to object
8. Rights in relation to automated decision making

4. What are my responsibilities?

All staff members have a responsibility to look after and maintain any data they have access to. Data relating to our colleagues and to our students must be treated with respect and be processed in line with our legal obligations. Data must only be processed if there is a justifiable reason, so if in doubt email the Charity's GDPR champion Emily Hartley-Heaven (emily.hartley-heaven@geckocommunity.org.uk)

The biggest difficulty to maintain is paper based reports. If you have printed any paperwork that contains student or staff data, then it is your responsibility to ensure the paper cannot:

1. be accessed by anyone who should not have access to it
2. is stored safely and securely
3. is destroyed correctly ensuring no loss of data.
4. who should I talk to for more information?

If you need any further information, then please contact your head of department, or contact the GDPR champion Emily Hartley-Heaven (emily.hartley-heaven@geckocommunity.org.uk)

5. What do I do if I suspect some data has been lost?

If you suspect there has been any data, accessed or lost that contains any of the categories under data protection, then it is important to notify as quickly as you can.

First you must always contact GDPR champion Emily Hartley-Heaven

- Email emily.hartley-heaven@geckocommunity.org.uk
- Telephone 07753 191991

If Emily is not available then contact the Data Protection Officer Piers Hartley by emailing piers.hartley@geckocommunity.org.uk 07717 334197. Once notification has been made the following process will be followed.

Contact the Data Protection Officer – piers.hartley@geckocommunity.org.uk within 48 hours

Notify Third Parties within 120 hours

Evaluation & Response to be presented by DPO

Breach Severity Assessment by DPO

Recovery Plan provided by DPO within 70 hours

Notify Information Office (ICO) within 72 hours

Notify Affected Individuals within 96 hours

Update ICO if required

6. Glossary of terms:

- GDPR – General Data Protection Regulations
- DP – Data Protection
- Charity – Fareham Charity
- Charity Personnel – Any Charity employee or contractor who has been authorised to access any of Our Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Charity.
- Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.
- Data Protection Officer – The Data Protection Officer is Piers Hartley, and can be contacted at: 07717 334197, piers.hartley@geckocommunity.org.uk
- ICO – the Information Commissioner's Office, the UK's data protection regulator.
- Personal Data – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.
- Processing – Any collection, use of storage of Personal Data whether on the Charity's information security systems or in paper form.
- Special Categories of Personal Data - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

Data Protection Policy

1. Overview

Gecko Community holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions within this policy:

- Business Purposes:
    - Personnel, administrative, financial, regulatory, payroll and business development purposes. o Compliance with our legal, regulatory and corporate governance obligations and good practice
    - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
    - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
    - Investigating complaints
    - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
    - Monitoring staff conduct, disciplinary matters o Marketing our business
    - Improving services
- Special Category
    - Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.
- Special Categories of Personal Data
    - 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.

2. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

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

3. Who is responsible for this policy?

The Charity's Data Protection Officer, has overall responsibility for the day-to-day implementation of this policy.

4. Our procedures

4.1 Fair and lawful processing

Gecko Community's employees and associates 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.

4.2 Responsibilities

The Data Protection Officer's responsibilities:

- 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 clients and employees who wish to know what data is being held on them by Gecko Community
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Gecko should inform shortlisted candidates that online searches may be done as part of due diligence checks.

Responsibilities of the IT Manager/Head of Technical Services

- Ensure all systems, services, software 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 Charity is considering using to store or process data

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of the MIS Manager

- Addressing data protection queries from clients and/or organisations that deal directly with the personal or sensitive data of our student body.
- Coordinating with the DPO to ensure all MIS initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of the HR Manager

- Addressing data protection queries from clients and or organisations that deal directly with the personal data of our staff teams.
- Coordinating with the DPO to ensure all HR initiatives adhere to data protection laws and the company's Data Protection Policy

General Responsibilities

- All Gecko personnel must comply with this policy.
- Gecko Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.
- Gecko Personnel must not release or disclose any Personal Data: outside the Charity; or
- inside the Charity to Gecko Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

• Gecko personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other Gecko Personnel who are not authorised to see such Personal Data or by people outside the Charity.

4.3 The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.
- Our Terms of Business contains a Privacy Notice to clients on data protection. The notice: Sets out the purposes for which we hold personal data on customers and employees
    - Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
    - Provides that customers have a right of access to the personal data that we hold about them

5. Special category personal data

In most cases where we process special category 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.

6. Accuracy and relevance

We will ensure that any personal data 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 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 you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

7. 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 contact Emily Hartley-Heaven so that they can update your records.

8. Data security

You must keep 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.

8.1 Storing data securely

8.1.1 Physical data storage:

• In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it. Printed data should be shredded when it is no longer needed.

8.1.2 Digital data storage:

• 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.

• 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 in line with the company's backup procedures

• Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

• All servers containing sensitive data must be approved and protected by security software and a strong firewall.

• All memory sticks and/or external hard drives used for storing personal or sensitive data, MUST be bit locker encrypted, with a strong password. This encryption will be implemented and maintained by IT.

9. Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention policy and guidelines.

10. Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer

personal data anywhere outside the UK without first consulting the Data Protection Officer. This includes both transference to 3rd parties and working on holiday. If you are in doubt contact the DPO for further clarification.

11. Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled to remove and/or amend, under applicable law.

12. Processing data in accordance with the individual's rights

You should 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.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

13. Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis. It will

cover:

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

Completion of training is compulsory.

14. GDPR provisions

As of the 25th of May 2018, new laws in Data Protection came into effect.
To ensure compliance with the new laws, the following provisions have been added and will be in effect as of the release of this policy.

14.1 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 queries must be asked when requesting data. The questions must be

asked and answers recorded within the data register, as well as being made accessible upon request:

What information is being collected?

Who is collecting it?

How is it collected?

Why is it being collected?

How will it be used?

Who will it be shared with?

Identity and contact details of any data controllers

Details of transfers to third country and safeguards

Retention period

14.2 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.

14.3 Justification for personal data

We will process personal data in compliance with all six data protection principles:

1. Fair and Lawful
2. Purposes
3. Adequacy

4. Accuracy
5. Retention
6. Rights

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

14.4 Consent

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

14.5 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.

14.6 Subject access requests

Individuals have the right under the GDPR to ask the Charity to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, the Charity will no longer be able to charge a fee for complying with the request.

Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

14.7 Right to be erased

A data subject may request that information held on them be deleted or removed, and any third parties who process or use that data must also comply with the request.

Right of erasure is a limited right where by individuals request the erasure of Personal Data concerning them where:

- the use of the Personal Data is no longer necessary;
- their consent is withdrawn and there is no other legal ground for the processing;
- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data has been unlawfully processed; and

- the Personal Data has to be erased for compliance with a legal obligation.

In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

14.8 Right of data portability

Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

Gecko Community will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the Charity's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which Gecko Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

14.9 Rights in relation to automated decision making and profiling

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where Gecko Community decides about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

Profiling happens where the Charity automatically uses Personal Data to evaluate certain things about an Individual.

Any Automated Decision Making or Profiling which the Charity carries out can only be done once the Charity is confident that it is complying with Data Protection Laws. If Gecko Personnel therefore wish to carry out any Automated Decision Making or Profiling Gecko Personnel must inform the Data Protection Officer.

Gecko Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

The Charity does not carry out Automated Decision Making or Profiling in relation to its employees.

14.10 Data protection impact assessments (DPIA)

The GDPR introduces a new requirement to carry out a risk assessment in relation

to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and ▪ the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

Where a DPIA reveals risks, which are not appropriately mitigated, the ICO must be consulted.

Where the Charity is launching or proposing to adopt a new process, product or service which involves Personal Data, the Charity needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The Charity needs to carry out a DPIA at an early stage in the process so that the Charity can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the Charity may have to carry out a Data Protection Impact

Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

All DPIAs must be reviewed and approved by the Data Protection Officer.

14.11 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.

14.12 International data transfers

No data may be transferred outside of the European Economic Area (EEA) without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

14.13 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.

15. Reporting breaches

Under the GDPR, Charity will be obliged to notify the ICO in the event of a Data Breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Notification must take place within 72 hours of the Charity becoming aware of the breach.

Gecko Community is obliged to notify any individuals affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination.

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

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are materia either in their own right or as part of a pattern of failures

Gecko Community is not obliged to notify the individuals affected where:

• there are technological and organisational protection measures (e.g. encryption);

• the Controller has taken action to eliminate the high risk; and

• it would involve disproportionate effort – in this case they must be informed some other way e.g. by a notice in newspapers.

However, the ICO will need to be notified, and may decide to alter the planned action of the Charity.

16. Contractors

If the Charity appoints a contractor who is a Processor of the Charity's Personal Data, Data Protection Laws require that the Charity only appoints them where the Charity has carried out sufficient due diligence and only where the Charity has appropriate contracts in place.

One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract where an organisation appoints a Processor must be in writing.

The Charity considers having appointed a Processor as engaging someone to perform a service for the Charity and as part of it they may get access to the Charity's Personal Data. Where the Charity appoints a Processor, the Charity, as Controller remains responsible for what happens to the Personal Data.

16.1 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or

general) of the Controller and under a written contract;

▪ to keep the Personal Data secure and assist the Controller to do so;

▪ to assist with the notification of Data Breaches and Data Protection Impact Assessments;

▪ to assist with subject access/individuals rights;

▪ to delete/return all Personal Data as requested at the end of the contract;

▪ to submit to audits and provide information about the processing; and

▪ to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

16.2 In addition, the contract should set out:

▪ The subject-matter and duration of the processing;

▪ the nature and purpose of the processing;

▪ the type of Personal Data and categories of individuals; and ▪ the obligations and rights of the Controller.

17. Compliance and monitoring

We take compliance with this policy very seriously. Failure to comply puts both you 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 in this policy, do not hesitate to contact the DPO.

18. Agreement

By signing this policy, you hereby agree to operate within the terms and conditions laid out within the policy

Your Name _____

Your Department _____ Date

_____

Copy of signed policy added to staff record: ☐ by _____on date _____

Data Retention Policy

1. Overview

This Retention Policy explains how Gecko Community complies with our legal obligation not to keep personal data for longer than we need it and sets out when different types of personal data will be deleted. In particular, it sets out details of the Charity's policies for the retention of Special Category personal data.

Data used by the Charity, must be protected and only processed where necessary in line with the guidance and legislation of the Data Protection Act 2018

Effective processing and data management is a team effort involving the participation and support of every Gecko Community employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable retention of data atGecko Community. These rules are in place to protect the students, employees andGecko Community. Inappropriate use exposes Gecko Community to potential data breach scenarios as well as legal action brought forth by data subjects.

3. Scope

This policy applies to the retention of personal and special category data, electronic and physical.

All employees, contractors, consultants, temporary, and other workers at Gecko Community and its subsidiaries are responsible for exercising good judgment regarding appropriate use/processing of data in accordance with Gecko Community policies and standards, local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, governors and other workers atGecko Community, including all personnel affiliated with third parties.

4. Policy

1.1 Gecko Community(the "Charity") must, in respect of its processing of personal data, comply with the Data Protection Act 2018, the General Data Protection Regulation 2016/679, and related legislation (together, "Data Protection Laws").

1.2 This Retention Policy should be read in conjunction with the Charity's Data Protection Policy, which sets out the Charity's overall approach to data protection matters and sets out the rationale for why a Retention Policy is required for personal data.

1.3 The Charity is under a legal obligation only to keep personal data for as long as the Charity needs it. Once the Charity no longer needs personal data, the Charity must securely delete it. The Charity recognises that the correct and lawful treatment of data will maintain confidence in the Charity and will provide for a successful working

environment.

1.4 This Policy applies to all Charity employees, consultants, contractors and temporary personnel hired to work on behalf of the Charity ("Gecko Personnel").

1.5 All Gecko Personnel with access to personal data must comply with this Retention Policy.

1.6 Please read this Retention Policy carefully. All Gecko Personnel must comply with it at all times. If you have any queries regarding this Retention Policy, please consult your manager and/ or the Data Protection Officer. You are advised that any breach of this Retention Policy will be treated seriously and may result in disciplinary action being taken against you.

1.7 Gecko Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any Gecko Personnel's contract of employment and the Charity reserves the right to change this Policy at any time. All Gecko Personnel are obliged to comply with this Policy at all times.

5. Data Retention Periods

1.8 The Charity has assessed the types of personal data that the Charity holds and the purposes the Charity use it for. The table below sets out the retention periods that the Charity has set for the different departments within the Charity, and the different types of data that they each hold.

1.9 If any member of Gecko Personnel considers that a particular piece of personal data needs to be kept for more or less time than the period set out in this policy, please contact the Data Protection Officer for guidance.

6. Retention periods for different categories of Data

Type of data	When will the Charity delete it (if manual)?	When will the Charity delete it (if electronic)	How will the Charity delete it (if manual)?	How will the Charity delete it (if electronic)?
Student Personal Details	7 Years	7 Years	Data Shredded	Data deleted from Database
Student Special Category Data	7 Years	7 Years	Data Shredded	Data deleted from Database

Staff Personal Data	6 Years	6 Years	Data Shredded	Data deleted from Database

Staff Special Category Data	6 Years	6 Years	Data Shredded	Data deleted from Database
Staff Criminal Record Data	6 Months	6 Months	Data Shredded	Data deleted from Database
Staff Bank Details	6 Months	6 Months	Data Shredded	Data deleted from Database
Visitor Personal Details	7 Years	7 Years	Data Shredded	Data deleted from Database
Supplier Details	7 Years	7 Years	Data Shredded	Data deleted from Database
Financial Records	7 Years	7 Years	Data Shredded	Data deleted from Database

7. Changes to this Policy

The Charity reserves the right to change this policy at any time.

Rights of Individuals Policy

1. Overview

The Charity's reputation and future growth are dependent on the way the Charity manages and protects Personal Data. All individuals have rights over their Personal Data and the Charity recognises the importance of having an effective Policy in place to allow individuals to exercise those rights in a way that is clear and easy for them. The Charity has therefore implemented this Rights of Individuals Policy to ensure all Gecko Personnel are aware of what rights individuals have over their Personal Data and how the Charity makes sure those rights can be exercised.

Gecko Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any GEcko Personnel's contract of employment and the Charity reserves the right to change this Policy at any time. All Gecko Personnel are obliged to comply with this Policy at all times.

2. About this policy

The Charity's Data Protection Policy is the Charity's fundamental policy which sets out the types of Personal Data that the Charity may be required to handle, as well as the Charity's legal purposes for doing so, and it sets out how the Charity complies with its obligations under Data Protection Laws.

This Policy explains how the Charity complies with its legal obligations to allow individuals to exercise their rights over their Personal Data. The Charity has a corresponding Rights of Individuals Procedure that sets out the process the Charity follows to deal with individuals exercising the rights set out in this Policy.

3. Scope

This Policy applies to all Gecko Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. Definitions

- Charity– Gecko Community
- Geco Personnel – Any Gecko Community employee or contractor who has been authorised to access any of Our Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Charity.
- Data Protection Laws – The General Data Protection Regulation (Regulation (EU)

2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

• Data Protection Officer – Data Protection Officer Piers Hartley can be contact on 07717 334197 or by emailing piers.hartley@geckocommunity.org.uk

• ICO – the Information Commissioner's Office, the UK's data protection regulator.

• Personal Data – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

• Processing – Any collection, use of storage of Personal Data whether on the Charity's information security systems or in paper form.

• Special Categories of Personal Data - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. Gecko personnel's obligations

This Policy sets out the rights that individuals have over their Personal Data under Data Protection Laws. If a member of the Gecko Personnel receives a request from an individual to exercise any of the rights set out in this Policy, that member of the Gecko Personnel must:

• inform the Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request;

• tell the Data Protection Officer what the request consists of, who has sent the request and provide the Data Protection Officer with a copy of the request;

• not make any attempt to deal with, or respond to, the request without authorisation from the Data Protection Officer.

6. What rights do individuals have over their personal data?

6.1 Right of access (subject access requests)

Individuals have the right to ask the Charity to confirm the Personal Data about them that the Charity is holding, and to have copies of that Personal Data (commonly known as a Subject Access Request or SAR) along with the following information:

The purposes that the Charity has their Personal Data for;

- the categories of Personal Data about them that the Charity has;
- the recipients or categories of recipients that their Personal Data has been or will be disclosed to;
- how long the Charity will keep their Personal Data;
- that they have the right to request that the Charity corrects any inaccuracies in their Personal Data or deletes their Personal Data (in certain circumstances, please see below for further information); or restrict the uses the Charity is making of their Personal Data (in certain circumstances, please see below for further information); or to object to the uses the Charity is making of their Personal Data (in certain circumstances, please see below for further information);
- that they have the right to complain to the ICO if they are unhappy about how the Charity has dealt with this request or in general about the way the Charity is handling their Personal Data;
- where the Personal Data was not collected from them, where the Charity got it from; and
- the existence of automated decision-making, including profiling (if applicable).

The Charity is not entitled to charge individuals for complying with this request. However, if the individual would like a further copy of the information requested, the Charity can charge a reasonable fee based on its administrative costs of making the further copy.

There are no formality requirements to make a SAR and it does not have to refer to data protection law, or use the words Subject Access Request or SAR. The Charity will monitor its incoming communications, including post, email, its website and social media pages to ensure that the Charity can recognise a SAR when it receives it.

The Charity is required to respond to a SAR within one month from the date the Charity receives it. If the SAR is complex or there are multiple requests at once, the Charity may extend this period by two further months provided that the Charity tells the individual who has made the SAR about the delay and the Charity's reasons for the delay within the first month.

The Data Protection Officer will reach a decision as to the complexity of the SAR and whether the Charity is entitled to extend the deadline for responding.

6.2 Right to rectification

Individuals have the right to ask the Charity to correct any Personal Data about them that the

Charity is holding that is incorrect. The Charity is then obliged to correct that Personal Data within one month (or two months if the request is complex).

When the individual tells the Charity their Personal Data is incomplete, the Charity is obliged to complete it if the individual asks the Charity to do so. This may mean adding a supplementary statement to their personal file for example.

If the Charity has disclosed the individual's inaccurate Personal Data to any third parties, the Charity is required to tell the individual who those third parties are and to inform the third parties of the correction where the Charity can.

When an individual asks the Charity to correct their Personal Data, the Charity is required to do so and to confirm this in writing to the individual within one month of them making the request.

6.3 Right to erasure (right to be forgotten)

Individuals have the right to ask the Charity to delete the Personal Data the Charity has about them in certain circumstances but this right is limited in scope and does not apply to every individual. The right to be forgotten applies when:

- the Personal Data is no longer necessary for the purpose the Charity collected it for;
- the individual withdraws consent and the Charity has no other legal basis to use their Personal Data:
- the individual objects to the Charity's processing and there is no overriding legitimate interest for continuing the processing;
- the Personal Data was unlawfully processed; and/or
- the Personal Data has to be erased to comply with a legal obligation.

If the Charity has disclosed the individual's deleted Personal Data to any third parties, the Charity is required to tell the individual who those third parties are and to inform the third parties to delete the Personal Data where the Charity can. When an individual asks the Charity to delete their Personal Data, the Charity is required to do so and to inform the individual in writing within one month of them making the request that this has been done.

6.4 Right to restrict processing

Individuals have the right to "block" or "suppress" the Charity's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the Charity to verify the accuracy of the Personal Data;
- the processing is unlawful and the individual opposes the deletion of the Personal Data and requests restriction instead;
- the Charity no longer needs the Personal Data for the purposes the Charity collected it for, but the Charity is required by the individual to keep the Personal Data for the establishment, exercise or defense of legal claims;
- the individual has objected to the Charity's legitimate interests, for a period enabling the Charity to verify whether its legitimate interests override their interests.

If the Charity has disclosed the individual's restricted Personal Data to any third parties, the Charity is required to tell the individual who those third parties are and to inform the third parties about the restriction where the Charity can.

When an individual asks the Charity to restrict its processing of their Personal Data, the Charity is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

6.5 Right to data portability

Individuals have the right to obtain from the Charity a copy of their own Personal Data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

The right to data portability only applies when:

- the individual provided the Charity with the Personal Data;
- the processing the Charity is carrying out is based on the individual's consent or is necessary for the performance of a contract; and
- the processing is carried out by automated means.This means that the right to data portability does not apply to personal data the Charity is processing on another legal basis, such as its legitimate interests.

The Charity is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that the Charity explains to the individual why it needs more time).

The individual also has the right to ask the Charity to transmit the Personal data directly to another organisation if this is technically possible.

6.6 Right to object

Individuals have the right to object to the Charity's processing of their Personal Data where:

- the Charity's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;
- the Charity is carrying out direct marketing to the individual; and/or
- the Charity's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

If an individual has grounds to object to the Charity's legitimate interests, the Charity must stop processing their Personal Data unless the Charity has compelling legitimate grounds for the processing which override the interests of the individual, or where the processing is for the establishment, exercise or defence of legal claims.

If an individual objects to direct marketing, the Charity must stop processing their Personal Data for these purposes as soon as the Charity receives the request. The Charity cannot refuse their request for any reason and cannot charge them for complying with it.

Before the end of one month from the date the Charity gets the request, the Charity must notify the individual in writing that the Charity has complied or intends to comply with their objections or that the Charity is not complying and the reasons why.

6.7 Rights in relation to automated decision making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:

- necessary for entering into or performing a contract between the Charity and the individual;
- required or authorised by Data Protection Laws; or
- based on the individual's explicit consent.

Automated decision making happens where the Charity makes a decision about an individual solely by automated means without any human involvement; and

Profiling happens where the Charity automatically uses Personal Data to evaluate certain things about an individual.

General Privacy Policy

1. Overview

This policy provides the guidance and definitions of the general privacy statements for Gecko Community. The policy covers details regarding Visitors and Suppliers.

2. Notice about how we use your personal information

We are the data controller of personal information about you. We are: Gecko Community. Our address is: Gecko Community, 44 Rodden Road, Frome, BA11 2AQ.

Our Data Protection Officer is Piers Hartley If you have any questions about this policy or the ways in which we use your personal information, please contact our GDPR champion Emily Hartley-Heaven (emily.hartley-heaven@geckocommunity.org.uk).

This privacy notice has been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018.

This policy breaks down the following categories:

- a visitor to the Charity
- one of our suppliers

As a visitor or supplier you have certain rights, including how to get a copy of any data relating to you, how to get it corrected or deleted, and how to complain. These rights are set out in more detail below.

Please note that on occasions we may process "special categories" of information about you. This is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.1 A visitor to the Charity

As a visitor to the Charity the following information is taken and used by the Charity. To aid you in understanding what data we take and why, please review the details below.

- the information we collect about you and why we collect it
- the legal basis on which we collect and use your personal information
- how long we keep your personal information
- how we share your personal information

- how we transfer your personal information outside Europe
- automated decisions we take about you

2.1.1 The information we collect about you and why we collect it:

As part of your visit to the Charity we store and use your personal details and information about your visit for the purposes of managing and operating the Charity.

2.1.2 The legal basis on which we collect and use your personal information

Except in the circumstances highlighted below, we process this information on the basis of our legitimate interests:

- we have a legitimate interest in wishing to interact with you to manage and operate effectively our Charity and to ensure that the Charity is safe and secure for all persons visiting; and
- We need to understand details of who is in the buildings and how we are able to communicate with them.

Where we are required by law to hold certain records, then we collect and hold those records to comply with that legal obligation.

2.1.3 How long we keep your personal information

By default, the Charity holds all records for 7 years.

2.1.4 How we share your personal information

By default, the Charity does not share information regarding its visitors with any third parties, however in certain circumstances we may have to share information with emergency and government services such as:

- Police Services
- Fire Services
- Ambulance Services
- Social Services

2.1.5 How we transfer your personal data outside Europe

We do not store or transfer your personal data outside Europe.

2.1.6 Automated decisions we take about you

We do not make automated decisions using this information.

2.2 One of our suppliers to the Charity

As a supplier to the Charity the following information is taken and used by the Charity. To aid you in understanding what data we take and why, please review the details below.

- the information we collect about you and why we collect it
- the legal basis on which we collect and use your personal information
- how long we keep your personal information
- how we share your personal information
- how we transfer your personal information outside Europe
- automated decisions we take about you

2.2.1 The information we collect about you and why we collect it

In order to engage and manage our suppliers, where you are a supplier (or where if it is a company, you are its representative) we collect and store your contact information and, where appropriate, your bank account details.

You may also be asked to provide details of your occupation and your CV.

In addition, where you visit a building we will collect and process the information set out in the “visitor to our Charity” section above.

2.2.2 The legal basis on which we collect and use your personal information

Except in the circumstances highlighted below, we process this information on the basis of our legitimate interests:

- we have a legitimate interest in engaging and managing our suppliers; and
- to be able to do so, we need to hold details of who those suppliers are.

Where we are required by law to hold certain records for health and safety purposes, then we hold those records to comply with that statutory obligation.

Where we hold your bank account details, we do so on the basis that it is necessary for us to perform our contract with you.

2.2.3 How long we keep your personal information

The Charity retains personal data for a maximum of 7 years after business conclusion.

Financial data is stored for a maximum of 6 years after business conclusion.

2.2.4 How we share your personal information

We may share the personal information that you give us with the following organisations (or types of organisation) for the following purposes.

- HMRC – for auditing and tax reviews
- Other suppliers - for references,

The Charity uses a cloud hosted financial system. The hosted system is located within the UK and has been bought in line with ISO27001.

We may also share your personal information with third parties who provide services to the Charity.

2.2.5 How we transfer your personal information outside Europe

We do not store or transfer your personal data outside Europe.

2.2.6 Automated decisions we take about you

We do not make automated decisions using this personal data.

3. Your rights

You have a number of rights over your personal information, which are:

- the right to make a complaint to the Information Commissioner's Office (ICO) if you are unhappy about the way your personal data is being used – please refer to the ICO's website for further information about this (https://ico.org.uk/);
- the right to ask us what personal information about you we are holding and to have access to a copy of your personal information;
- the right to ask us to correct any errors in your personal information;
- the right, in certain circumstances such as where our use of your personal information is based on your consent and we have no other legal basis to use your personal information, to ask us to delete your personal information;
- the right, in certain circumstances such as where we no longer need your personal information, to request that we restrict the use that we are making of your personal

information;

• the right, in certain circumstances, to ask us to review and explain our legitimate interests to you; and

• the right, where our use of your personal information is carried out for the purposes of an agreement with us and is carried out by automated means, to ask us to provide you with a copy of your personal information in a structured, commonly-used, machine-readable format.

4. Changes to our privacy policy

We keep our privacy policy under regular review and will update it from time to time to make sure it remains up-to-date and accurate.

Privacy Policy - Staff

1. Overview

We are the data controller of personal information about you. We are Gecko Community. Our address is: Gecko Community, 44 Rodden Road, Frome, BA11 2AQ.

Our Data Protection Officer is Piers Hartley. If you have any questions about this policy or the ways in which we use your personal information, please contact our GDPR champion Emily Hartley-Heaven (emily.hartley-heaven@geckocommunity.org.uk). Telephone 07753 191991

This privacy notice has been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018.

2. How we use your personal information

This notice sets out how we use your personal information as your employer or when you apply for a job with us and in particular:

- the information that you give us;
- the uses made of your personal information;
- the legal basis on which we collect and use your personal information;
- how long we keep your personal information:
- how we share your personal information;
- how we transfer your personal information outside of Europe; and
- your rights over your personal information.

3. The Information You Give Us

We will collect personal information from you when you apply for a job with us. This will include your: name; address; phone number; email; current employment details including job title, start and end dates, current salary, notice period, reason for leaving; all past employment details; education details; interests; whether you are related to any personnel of the Charity or Governing Body; references; special arrangement details for interview; equality monitoring information; criminal record details; Disclosure Barring Service check, including European Economic Area (EEA) check; Check of Barred List/List 99; Pre employment Health Questionnaire/Medical Report, Right to Work in the UK check.

We will collect personal information from you when you are a new starter and become an employee of the Charity. This will be your: name; marital status; previous surname(s); address; date of birth; occupation/department; type of employment; phone number; email addresses; NI

number; start date; next of kin and contact details; bank details; pension details; statement about employment; student loan details; offer letters; employment terms and conditions; changes to your terms and conditions; certifications/qualifications, training details, disciplinary, grievance, capability, job descriptions, sickness absences, maternity/paternity/adoption information; accidents and injuries at work; working time information; annual leave records; recruitment information; photo; payroll details; gender; flexible working; exit interviews; return to work notifications; parental leave request forms; appraisal/performance; bank account number; sort code; disqualification information; sickness absences; medical information; criminal conviction details.

4. The Uses Made of Your Personal Information

We will use your personal information set out above as follows:

- for the recruitment process and for carrying out pre-employment checks;
- for safeguarding students;
- for checking your identity and right to work in UK;
- for checking your qualifications;
- to keep an audit trail of the checks we have made and our relationship with you in case of employment claims;
- to set up payroll and pension and to reimburse expenses;
- for dealing with HMRC;
- for communicating with you, including for marketing purposes;
- for carrying out our role as your employer or potential employer.

We treat your personal information with confidentiality and we do not use it for any other purposes.

5. The Legal Basis on Which We Collect and Use Your Personal Information

We collect and use your personal information on the basis that it is necessary for performing our employment contract with you, or it is necessary to take steps before entering into the contract with you. We also collect and use your personal information on the basis that we need to do so in order to comply with our legal obligations.

6. How long we keep your information

We will not keep your personal information for longer than we need it for the purposes we have explained above.

When you are an employee, we will keep your personal information for as long as you work with us and then after you leave, we will keep your personal information for 6 years.

7. How we share your information

We may also share your personal information with third parties who provide services to the Charity.

Organisation / type of organisation and service provision.

8. How we transfer your information outside of Europe

All HR data is stored either on premises or within our UK hosted data centres. We do not store or transfer your personal data outside of Europe.

9. Your Rights over your personal information

You have a number of rights over your personal information, which are:

• the right to make a complaint to the Information Commissioner's Office (ICO) if you are unhappy about the way your personal data is being used – please refer to the ICO's website for further information about this (https://ico.org.uk/);

• the right to ask us what personal information about you we are holding and to have access to a copy of your personal information;

• the right to ask us to correct any errors in your personal information;

• the right, in certain circumstances such as where our use of your personal information is based on your consent and we have no other legal basis to use your personal information, to ask us to delete your personal information;

• the right, in certain circumstances such as where we no longer need your personal information, to request that we restrict the use that we are making of your personal information;

• the right, in certain circumstances, to ask us to review and explain our legitimate interests to you; and

• the right, where our use of your personal information is carried out for the purposes of an agreement with us and is carried out by automated means, to ask us to provide you with a copy of your personal information in a structured, commonly used, machine-readable format.

10. Changes to our privacy Policy

We keep our privacy policy under regular review. Any changes we make to our privacy policy in the future will be notified to you by email.

Privacy Policy - Students

1. Overview

We are the data controller of personal information about you. We are Gecko Community. Our address is: Gecko Community, 44 Rodden Road, Frome, BA11 2AQ.

Our Data Protection Officer is Piers Hartley. If you have any questions about this policy or the ways in which we use your personal information, please contact our GDPR champion Emily Hartley-Heaven (emily.hartley-heaven@geckocommunity.org.uk). Telephone 07753 191991

This privacy notice has been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018.

2. How we use your personal information

This notice sets out how we use your personal information as a Charity or when you apply for a course with us and in particular:

- the information that you give us;
- the uses made of your personal information;
- the legal basis on which we collect and use your personal information;
- how long we keep your personal information:
- how we share your personal information;
- how we transfer your personal information outside of Europe; and
- your rights over your personal information.

3. The Information You Give Us

We will collect personal information from you when you apply for a course with us. This may include your: name; address; phone number; email; current and former education details including course title, start and end dates, grades achieved; interests; whether you are related to any personnel of the Charity or Governing Body; references; special arrangement details for attendance; equality monitoring information; criminal record details.

4. The Uses Made of Your Personal Information

We will use your personal information set out above as follows:

- for the student recruitment process;
- for safeguarding other students;

- for checking your identity and right to study in the UK;
- for checking your qualifications;
- to keep an audit trail of the checks we have made and our relationship with you in case of any claims;
- for communicating with you, including for marketing purposes;
- for carrying out our role as your educator.

We treat your personal information with confidentiality and we do not use it for any other purposes.

5. The Legal Basis on Which We Collect and Use Your Personal Information

We collect and use your personal information on the basis that it is necessary for performing our education contract with you, or it is necessary to take steps before entering into the contract with you. We also collect and use your personal information on the basis that we need to do so in order to comply with our legal obligations.

Where we collect your special category personal information, we do this on the basis that it is necessary for the purposes of carrying out our obligations in the field of education law. Special categories of personal data are personal data that reveal a person's racial or ethnic origin, political opinions, religions or philosophical beliefs, genetic data (i.e. information about their inherited or acquired genetic characteristics, information about physical, physiological or behavioural characteristics (such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal records).

6. How long we keep your information

We will not keep your personal information for longer than we need it for the purposes we have explained above.

When you are a student, we will keep your personal information for as long as you study with us and then after you leave, we will keep your personal information for 6 years. Under education law we must retain your name, unique learner number and study from and to dates, for up to 90 years.

7. **How we share your information**

We may also share your personal information with third parties who provide services to the Charity.

8. How we transfer your information outside of Europe

All student data is stored either on premises or within our UK hosted data centres. We do not store or transfer your personal data outside of Europe.

9. Your Rights over your personal information

You have a number of rights over your personal information, which are:

• the right to make a complaint to the Information Commissioner's Office (ICO) if you are unhappy about the way your personal data is being used – please refer to the ICO's website for further information about this (https://ico.org.uk/);

• the right to ask us what personal information about you we are holding and to have access to a copy of your personal information;

• the right to ask us to correct any errors in your personal information;

• the right, in certain circumstances such as where our use of your personal information is based on your consent and we have no other legal basis to use your personal information, to ask us to delete your personal information;

• the right, in certain circumstances such as where we no longer need your personal information, to request that we restrict the use that we are making of your personal information;

• the right, in certain circumstances, to ask us to review and explain our legitimate interests to you; and

• the right, where our use of your personal information is carried out for the purposes of an agreement with us and is carried out by automated means, to ask us to provide you with a copy of your personal information in a structured, commonly used, machine-readable format.

10. Changes to our privacy Policy

We keep our privacy policy under regular review. Any changes we make to our privacy policy in the future will be notified to you by email.

Personal Data Breach Notification Policy

1. Overview

The Charity's reputation and future growth are dependent on the way the Charity manages and protects Personal Data. As an organisation that collects and uses Personal Data, the Charity takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The Charity's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected. The Charity has therefore implemented this Policy to ensure all Charity Personnel are aware of what a Personal Data reach is and how they should deal with it if it arises.

Charity Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any Charity Personnel's contract of employment and the Charity reserves the right to change this Policy at any time. All Charity Personnel are obliged to comply with this Policy at all times.

2. About this policy

This Policy explains how the Charity complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals. The Charity has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the Charity deals with and records Personal Data breaches.

3. Scope

This Policy applies to all Charity Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. Definitions

Charity – Gecko Community

Charity Personnel – Any Gecko Community employee or contractor who has been authorised to access any of the Charity's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Charity.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – The Data Protection Officer is Piers Hartley: piers.hartley@geckocommunity.org.uk, Telephone 07717 334197.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Personal Data – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

Special Categories of Personal Data - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. What is a personal data breach?

The Charity takes information security very seriously and the Charity has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The Charity has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

A Personal Data breach could include any of the following:

- loss or theft of Personal Data or equipment that stores Personal Data;
- loss or theft of Personal Data or equipment that stores the Charity's Personal Data from a Charity supplier;
- inappropriate access controls meaning unauthorised Charity Personnel can access Personal Data;
- any other unauthorised use of or access to Personal Data;
- deleting Personal Data in error;
- human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);
- hacking attack;
- infection by ransom ware or any other intrusion on our systems/network;
- 'blagging' offenses where information is obtained by deceiving the organisation who holds it; or
- destruction or damage to the integrity or accuracy of Personal Data.

A Personal Data breach can also include:

- equipment or system failure that causes Personal Data to be temporarily unavailable;
- unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;
- inability to restore access to Personal Data, either on a temporary or permanent basis; or
- loss of a decryption key where Personal Data has been encrypted because this means the Charity cannot restore access to the Personal Data.

6. Reporting a data breach

Charity Personnel must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not Charity Personnel thinks a breach has occurred or is likely to occur. This allows the Charity to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the Charity.

If Charity Personnel discover a Personal Data breach outside working hours, Charity Personnel must notify it to the Charity's Data Protection Officer as soon as possible.
Charity Personnel may be notified by a third party (e.g. a supplier that processes

Personal Data on the Charity's behalf) that they have had a breach that affects Charity

Personal Data. Charity Personnel must notify this breach to the Charity's Data Protection Officer and the Charity's Data Breach Notification Procedure shall apply to the breach.

7. Managing a personal data breach

There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

1. Containment and recovery
2. Assessment of on-going risk
3. Notification
4. Evaluation and response

At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

8. Containment and recovery

An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected, then it will be added to the Charity's Data Breach Register and no further action will be taken.

If the Personal Data breach may impact on the rights and freedoms of the individuals affected, then the Charity will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the Charity's Data Breach Notification Procedure. This will include consideration of:

• whether there are any other people within the Charity who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

• what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

• whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer.

All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

9. Assessment of ongoing risk

As part of the Charity's response to a Personal Data breach, once the breach has been contained the Charity will consider the on-going risks to the Charity and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the Charity's Data Breach Notification Procedure.

10. Notification

Under Data Protection Laws, the Charity *may* have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

Any notification will be made by the Data Protection Officer following the Charity's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the Charity becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore imperative that Charity Personnel notify all Personal Data breaches to the Charity in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the Charity will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the Personal Data breach relates to a temporary loss of availability of the Charity's systems, the Charity does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The Charity does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case by case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, the Charity may need to carry out in-depth investigations. In these circumstances, the Charity will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When the Charity notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the Charity has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

The Charity may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

11. Evaluation and response

It is important not only to investigate the causes of the breach but to document the breach and

evaluate the effectiveness of the Charity's response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of the Charity's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

Any remedial action such as changes to the Charity's systems; policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

Rights of Individuals Procedure

1. Overview

The Charity's reputation and future growth are dependent on the way the Charity manages and protects Personal Data. All individuals have rights over their Personal Data. This Rights of

Individuals Procedure must be read in conjunction with the Charity's Rights of Individuals Policy. It explains the process the Charity follows to comply with its legal obligations to allow individuals to exercise their rights over their Personal Data which are detailed in the Rights of Individuals Policy.

Charity Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any Charity Personnel's contract of employment and the Charity reserves the right to change this Policy at any time. All Charity Personnel are obliged to comply with this Policy at all times.

2. About this policy

The Charity's Data Protection Policy is the Charity's fundamental policy which sets out the types of Personal Data that the Charity may be required to handle, as well as the Charity's legal purposes for doing so, and it sets out how the Charity complies with its obligations under Data Protection Laws.

This Procedure explains the process the Charity has in place to ensure that the Charity complies with its legal obligations to allow individuals to exercise their rights over their Personal Data. The Charity has a corresponding Rights of Individuals Policy that sets out what those rights are and explains Charity Personnel's obligations in relation to ensuring that the Charity meets its obligations in this area.

3. Scope

This Policy applies to all Charity Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. Definitions

- **Charity** – Gecko Community

• **Charity Personnel** – Any Charity employee or contractor who has been authorised to access any of Our Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Charity.

•**Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and

privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

• **Data Protection Officer** –The Data Protection Officer is Piers Hartley: piers.hartley@geckocommunity.org.uk, Telephone 07717 334197

• **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

• **Personal Data** – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

• **Special Categories of Personal Data** - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. How do we allow individuals to exercise their rights under data protection laws?

5.1 Right of access (subject access requests)

5.1.1 Individuals have the right to ask the Charity to confirm the Personal Data about them that the Charity is holding, and to have copies of that Personal Data (commonly known as a Subject Access Request or SAR).

5.1.1 If a member of the Charity personnel receives a request from an individual to access or to receive a copy of their personal data, the following procedure will be followed:

5.1.1.1 the Charity personnel must forward or report the request to the Data Protection Officer as soon as they receive it. A request from an individual does not have to be in a particular format, for example it does not have to be in writing. If the request is not made in writing (e.g. it is taken over the telephone) best practice is that the Charity asks the individual to confirm in writing so it can ensure it is complying correctly with the request. If they do not wish to do this, then please confirm the request in writing and ask them to indicate if there are any inaccuracies. Please note that the Charity can no longer charge a fee for responding to these requests unless a second or subsequent copy of the Personal Data is requested (in which case the Charity can charge its administrative costs) or the request is unfounded or excessive (see heading 6 ‘Are there any requests the Charity does not have to respond to?’ below);

5.1.1.2 the Data Protection Officer will diarise the date the request as received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out under sub heading 7 ‘Response Times’ below), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

5.1.1.3 within 10 working days of receipt, the Data Protection Officer will decide whether any further information is needed from the individual to clarify the identity of the individual or to understand the request and will ask the individual for any further information that is needed as soon as possible;

5.1.1.4 if further information is required, no action will be taken until the further information has been received from the individual;

5.1.1.5 once the further information has been received and/or the Charity is satisfied that it knows what has been asked for, the Charity will begin locating the individual’s Personal Data;

5.1.1.6 depending on who the individual is, this may involve locating staff files, student files, information on parents, notes, minutes, correspondence and other relevant documents containing Personal Data either on the Charity’s information systems, or in the Charity’s structured paper filing systems. The Data Protection Officer will let Charity Personnel know what searches they need to carry out;

5.1.1.7 once the Charity has located all the Personal Data of the individual, the Data Protection Officer will review it and decide whether any of the Personal Data does not need to be disclosed as there are exemptions which may apply;

5.1.1.8 once the Charity has decided what the Charity is going to provide to the individual, the Charity will respond providing copies of the Personal Data, which, if the request is made electronically, shall be provided in a commonly used electronic form; and

5.1.1.9 if the Charity fails to do this within one month of the date the Charity receives the request, the Charity will ensure that it has contacted the individual before the deadline to explain what the Charity has done so far and when the Charity will get back to them with their Personal Data.

5.2 **Right to rectification**

5.2.1 If a member of the Charity Personnel receives a request from an individual to correct their Personal Data, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as so as they receive it;

• the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in subheading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

• the Charity will then locate the Personal Data concerned and verify whether it is incorrect or incomplete and will correct it or complete it as soon as possible; • the Charity will ascertain whether the Charity has disclosed the incorrect Personal Data to any third parties and, if so, the Charity will contact those third parties as soon as possible to tell them to correct the Personal Data;

• the Data Protection Officer will decide whether the Charity needs to keep a copy of the original Personal Data for evidence reasons or otherwise; and • the Charity will confirm to the individual in writing within one month of the date of their request that the Charity has complied with the request.

5.3 Right to erasure (right to be forgotten)

5.3.1 If a member of the Charity Personnel receives a request from an individual to delete their Personal Data, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

• the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in sub heading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the

request in order to track its progress;

• the Data Protection Officer will reach a decision as to whether the right to be forgotten applies;

• if the right to be forgotten does apply, the Data Protection Officer will decide whether the Charity is required to keep any parts of the Personal Data for evidence reasons and, if so, this Personal Data will be excluded from the request;

• the Charity will then securely delete all the Personal Data about that individual that the Charity has which is not excluded. This will include securely shredding all hard copy documents and ensuring that computer records are securely deleted from the Charity's information systems in line with the processes detailed in the Charity's Data Retention Policy;

• the Charity will ascertain whether it has disclosed the deleted Personal Data to any third parties and, if so, the Charity will contact those third parties as soon as possible to tell them to delete the Personal Data; and

• the Charity will confirm to the individual in writing within one month of the date of their request that the Charity has complied with the request.

5.4 Right to restrict processing

5.4.1 If a member of the Charity Personnel receives a request from an individual to restrict the Charity's use of their Personal Data, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

• the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in sub heading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

• the Data Protection Officer will reach a decision as to whether the right to restrict processing applies;

• if the right to restrict processing does apply, the Charity will action the request as soon as possible and ensure that the Charity no longer uses the individual's Personal Data in the way they have objected to. This may include moving documents to folders where they can no longer be accessed, removing details from files and locking paper files away;

• the Charity will ascertain whether the Charity has disclosed the Personal Data to any third parties and, if so, the Charity will contact those third parties as soon as possible to tell them to stop using the Personal Data in the restricted way;

and

• the Charity will confirm to the individual in writing within one month of the date of their request that the Charity has complied with the request.

5.5 Right to data portability

5.5.1 If a member of the Charity Personnel receives a request from an individual to provide a copy of their Personal Data in a structured, commonly-used and machine-readable format, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as soon as they receive it; • the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in subheading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

• the Data Protection Officer will reach a decision as to whether the right to data portability applies and to which subset of the individual's Personal Data it applies; and

• if the right to data portability does apply, the Charity will action the request as soon as possible. This will include creating an electronic copy of the individual's Personal Data which can be transferred to another organisation if the individual asks the Charity to.

5.6 Right to object

5.6.1 If a member of the Charity Personnel receives an objection from an individual to the

Charity's processing of their Personal Data, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

• the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in subheading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

• the Data Protection Officer will reach a decision as to whether the right to object applies;

• if the right to object does apply, the Charity will action the request as soon as possible. This may include suppressing the individual from the Charity's direct marketing lists, or stopping the processing of Personal Data that has been objected to; and

• the Charity will write to the individual within one month of the date of their request to tell them either that the Charity has complied with, or intends to comply with, their request or that the Charity has not complied and the reasons why the Charity has not complied.

5.7 Rights in relation to automated decision making

5.7.1 If a member of the Charity Personnel receives an objection from an individual to an automated decision that the Charity has made about the individual which produces legal effects concerning them or similarly significantly affects them, the following procedure will be followed:

• the Charity Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

• the Data Protection Officer will diarise the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in subheading 6 'Are there any requests the Charity does not have to respond to?'), and send weekly chasers to all Charity Personnel involved in dealing with the request in order to track its progress;

• the Data Protection Officer will reach a decision as to whether the right to intervene in the automated decision making applies;

• if the right to intervene does apply, the Charity will action the request as soon as possible. This will involve reviewing the automated decision-making process, reviewing the decision that was made, having a Charity Personnel consider whether the decision needs to be retaken and allowing the individual to give their view on the decision; and

• the Charity will write to the individual within one month of the date of their request to tell them what the outcome of the Charity's review is. Automated decision making happens where the Charity makes a decision about an individual solely by automated means without any human involvement; and Profiling happens where the Charity automatically uses Personal Data to evaluate certain things about an individual.

5. Are there any requests the Charity does not have to respond to?

If the request the Charity receives from an individual is unfounded or excessive then the Charity may either:

- refuse to action the request; or
- charge a reasonable fee taking into consideration the Charity's administrative costs of providing the information or taking the action requested.

Any decisions in relation to not actioning the request or charging a fee shall be made by the Data Protection Officer.

6. Response Times

All requests set out above must be responded to within a month unless the request is complex in which case the period may be extended up to a further two months. Any decision in relation to whether the request is complex is to be made by the Data Protection Officer who shall inform the individual making the request of the extension. Any notification of the extension to the individual shall be made within the initial one-month period and shall give reasons for the delay.

If the Charity is not going to action the request made by an individual, the Data Protection Officer shall communicate this to them within a month of receipt of the request. The communication shall include details of the Charity's reasons for not actioning the request and the ability of the individual to make a complaint to the ICO.

7. Legal Advice

Specialist external legal advice may be taken on the above, but this shall be the decision of the Data Protection Officer.

Data Breach Notification Procedure

1. Overview

Where there is a data breach within the Charity, it is a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to us.

This Procedure should be read in conjunction with our Data Breach Policy and Data Protection Policy. Our Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you are aware of the breadth of the concept of a data breach.

This Procedure should be followed by all staff. At all stages of this procedure, our Data Protection Officer and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our personal data.

2. Procedure

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

IDENTIFYING AND REPORTING A DATA BREACH
If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is Richard Bryant, and can be contacted at: 01329 815 200 during work hours, alternatively you can email him at piers.hartley@geckocommunity.org.uk. Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer. A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches *must* be reported. False alarms or even breaches that do not cause any harm to individuals or to the Charity should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place. We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, our Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that are breach has occurred that has led to personal data being compromised.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, our Data Protection Officer will notify management. If necessary, we will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the Charity and any individuals affected.

If our Data Protection Officer and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

THIS WILL BE DONE WITHIN 48 HOURS OF US BECOMING AWARE OF THE BREACH.

FORMULATING A RECOVERY PLAN

Our Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

THIS WILL BE DONE WITHIN 70 HOURS OF ASSESSING THE BREACH.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, we must notify the breach to the ICO within 72 hours of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy, and the notification will be made by our Data Protection Officer – please be aware that under no circumstances must you try and deal with a data breach yourself.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that under no circumstances must you try and deal with a data breach yourself.

In some circumstances, explained in our Data Breach Policy, we may not need to notify the affected individuals. Our Data Protection Officer will decide whether this is the case.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police
- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.

Note: We suggest that a time frame is included. We suggest a timeframe of 5 days. Please do amend this time frame as you see fit in terms of practicality and how quickly the Charity will complete this step.

CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED
We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our Data Protection Officer will consider whether we need to update the ICO about the data breach. THIS WILL BE CONSIDERED ON AN ONGOING BASIS.

EVALUATION AND RESPONSE
The key to preventing further incidents is to ensure that the Charity learns from previous incidents. It is extremely important to identify the actions that the Charity needs to take to prevent a recurrence of the incident. Our Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.

Policy prepared by Emily Hartley-Heaven: November 2021

Updated: November 2023
Emily Hartley-Heaven
Placement Coordinator and Safeguarding Lead

Renewal Date: November 2024