The Bikeability Trust

Data Protection Policy and Procedures

Introduction

This policy outlines how colleagues of the Bikeability Trust manage data within your role. It should be read in conjunction with the Data Protection Guidance document.

The Trust is committed to the protection of the personal data of employees and other individuals about whom it might hold information. The Trust recognises its obligations to UK data protection law which includes but may not be limited to the UK General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications Regulation (PECR) and the Data Protection Act 2018 as its statutory responsibility relating to data handling and processing.

To this end every individual handling data collected or administered by the Trust must take responsibility and have due consideration for its appropriate use in line with this policy.

This policy applies to all individuals for whom we may process personal data including employees, volunteers and other relevant parties (hereinafter referred to as 'colleagues'). Any deliberate breach of this policy may lead to disciplinary action being taken, or access to Trust facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

This data protection policy ensures the Bikeability Trust:

- Complies with data protection law and follows good practice
- Protects the rights of colleagues, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

This Policy should also be read in conjunction with:

- Data Protection Impact Assessment
- Fundraising policy
- Core services manual

The Bikeability Trust has a responsibility to ensure anyone who comes into contact with the Trust understands how we process their data. We set this out in our Privacy Statement Privacy Policy | Bikeability.

Relevant data protection law

The UK General Data Protection Regulation (GDPR) is the version of the EU law that was established after Brexit. It works alongside the Data protection Act 2018 (DPA).

The DPA describes how organisations must collect, handle and store personal data. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The DPA is underpinned by the following seven principles. According to these principles, personal data must be

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- used in a way that that ensures we can be held accountable for our decisions

The principles are a series of obligations which lie at the heart of our compliance. They include the obligation to be transparent about our intentions. We achieve this using our privacy notices to ensure we inform individuals of our intended processing activities.

We must be purpose driven and only collect the data we need to achieve those objectives.

We must endeavour to keep data up to date and ensure we only process accurate data.

We must decide how long to retain data and delete it at the appropriate time.

We must keep data safe and secure which includes every employee's handling of personal data

We must keep accurate records of our processing activities so that we are accountable for our actions.

Responsibilities

This policy applies to all operations of the Bikeability Trust, and to all Bikeability trustees, employees and associates. It applies to all data the Trust holds relating to identifiable individuals, even when technically these data fall outside the DPA. This can include names of individuals, postal and email addresses, telephone numbers, and any other information relating to individuals.

1. Employees

The Trust holds various items of personal data about its employees which are detailed in the Privacy Notice. All personal information from recruitment to onboarding to ongoing employment is held on the Breathe HR system with privacy and security key features of the system. Employees must ensure that all personal data provided to the Trust in the process of employment is accurate and up to date. They must ensure that changes of address etc are updated.

In the course of day to day working it is likely that employees will process individual personal data. Prior to handling any data, employees are required to have completed training in data protection. In addition, employees must maintain a current understanding of what is required of them under Data Protection law. The Trust requires all staff to undertake e-learning on Information Security and the UK GDPR.

When handling personal data, employees are required to follow the guidance set out in the Data Protection Guidance.

We may undertake DBS checks on certain individuals that work for the Trust. In such circumstances we will be processing criminal records in accordance with UK GDPR Art.10 regardless of the outcome of such checks. Therefore, we have identified the appropriate conditions for processing such data and have an appropriate policy document in force.

2. Managers

Managers must ensure that employees handling data in the course of their roles have undertaken the appropriate training, are processing data within the frameworks agreed and following the guidance set out in the Data Protection Guidance document.

Managers will conduct regular audits of their areas to identify weaknesses in information security. Where weaknesses are found, the Chief Executive Officer should be notified so that action can be taken promptly.

3. Directors

The Directors are required to demonstrate ownership of this policy and to communicate its values across the Trust. This accountability cannot be delegated, however, operational aspects of data protection management may be delegated to others. They must gain assurance that these responsibilities are being fulfilled and ensure resources are available to fulfil the requirements of this policy and associated procedures. They have overall accountability for the strategy of the Trust and are responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Trust. We have appointed a GDPR data protection officer to ensure the directors have adequate advice and guidance.

4. The Information Security and Governance Lead

The Chief Executive Officer provides the lead for Information Security and Governance and is responsible for the practical implementation of data protection legislation across the Trust and ensures that the principles of data protection law are upheld. They must provide assurance to the directors that the Trust's obligations under data protection law are met and advise the wider Trust on day to day data protection issues. The Chief Executive Officer will also hold responsibility for:

- Keeping the trustees updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related polices, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from employees and anyone else covered by this policy
- Dealing with requests from individuals to see the data the Trust holds about them
- Checking and approving any contracts or agreements with third parties that may handle the Trust's sensitive data
- Ensuring all systems, services and equipment for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly

- Evaluating any third-party services the Trust is considering using to store or process data (e.g. cloud computing services)
- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- Where necessary, working with other colleagues to ensure marketing initiatives abide by data protection principles.

Compliance

1. Respecting Individuals' Rights

The UK GDPR sets out a series of rights for individuals. Employees planning data processing activities must record how these rights are addressed. The Data Protection Guidance details the rights and the company's standardised processes to meet these individual rights.

2. Processing Special Categories of Data

The company will only process special categories of data linked to individuals, such as:

- racial or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature
- trade organisation membership
- sexual life or sexual orientation
- genetic or biometric data

Where such data is processed, we may use the consent of the individual. However, in certain other circumstances we use an alternative condition linked with a UK GDPR Art.9 condition. Some of these conditions require further conditions to be lawful. We may use an appropriate policy document under some circumstances.
We will process personal data with the consent of individuals except for where:

- there is another legal basis on which to process this data
- this is not required by law
- the information is required to protect individual health in an emergency.

In other circumstances we may process data using the legitimate interests of the Trust. In order for this to be lawful we will ensure that there is a reasonable expectation of such processing, that there is no real alternative and that the individual may object to such activity.
This data may be analysed in broad terms where no direct link to an individual can be made.

3. Processing Health Related Data

The Trust will process information relating to individuals' physical or mental health in order to comply with health and safety, occupational health or other legal obligation and to undertake an assessment of colleague capability.

4. Subject Access Requests

The Bikeability Trust

The Data Protection Guidance details the procedures on how Subject Access Requests must be handled. As standard, the Trust does not charge to comply with access requests and will refuse manifestly unfounded or excessive requests. Such requests will be handled in accordance with the guidance of the ICO.

5. Data Breaches

The Trust will put in place processes to detect data breaches including audits and other appropriate processes. Where a colleague discovers a data breach they must report this to dpo@bikeabilitytrust.org as soon as possible and in any case within 24 hours.

If a colleague has been made aware of a data breach, they should follow the Security Incident Procedure

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where there is a high risk to the rights and freedoms of individuals they shall also be notified directly. Before any action is taken, the DPO should be consulted for their opinion as to whether the incident has reached the threshold for a report to the ICO.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. A data security breach can happen for a number of reasons:

- loss or theft of data or equipment
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking attack
- deception of the company.

Detecting a data breach or the potential of a data breach can happen in a variety of ways. The table below identifies some of the methods of detection and processes for handling such detections.

Detection Method	Action for potential breach	Action for actual breach
Colleague Detection	If you think you have identified a potential for data security to be breached you must immediately inform the dpo@bikeabilitytrust.org . They may immediately cease processing this data until the potential for breach is resolved based upon an assessment of the risk to individuals privacy.	Immediately report the matter to the dpo@bikeabilitytrust.org- isolating any potential for further breach where appropriate. The Directors should follow the required process from here.

Accidental Breach (such as loss of laptop)	If there is a high likelihood of this breach happening you should immediately adjust your processes and procedures to reduce the likelihood. Always ensure data is secured and encrypted as detailed in the information security section of this handbook. Consult the dpo@bikeabilitytrust.org where appropriate.	Immediately report the matter to the dpo@bikeabilitytrust.org- isolating any potential for further breach where appropriate.
Audit or assessment	The company conducts termly data audits of its spaces and IT infrastructure - these may highlight weaknesses in the company's information security and should be responded (with advice from the Directors) in a timely manner to ensure data privacy of individuals.	Immediately report the matter to the dpo@bikeabilitytrust.org - isolating any potential for further breach where appropriate.
Complaint from either an individual, organisation or legal representative	Where there is a risk of complaint arising from the processing of data that may raise to being a legal matter processing must immediately cease, the Directors must be advised and comprehensive guidance sort from the Information Commissioner's Office.	Immediately report the matter to the Directors who should follow the required process from here.

The Trust takes all data breaches seriously and will investigate all potential and actual data security breaches.

The Directors will implement an incident response plan in such circumstances.

Information Security

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Executive Officer

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by colleagues in accordance with statutory, regulatory, contractual and Trust policy requirements.

The Trust has a number of platforms for securely storing data online including:

- BreatheHR
- Link
- Microsoft Office 365

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. To achieve this, the Trust and colleagues must:

- use storage on the Trust's network or approved platform
- apply password protection on all files containing personal data when being shared with other colleagues
- use secure platforms for processing data
- maintain up to date antivirus and malware systems
- have adequate firewalls
- ensure secure destruction of IT equipment.

Colleagues are not permitted to use external storage devices such as external hard drives, memory sticks, pen drives etc. for storage of any Trust data other than for transfer of photos and data whilst on Trust premises.

International transfers of personal data must only be made under certain circumstances. The UK has a strict transfer regime that protects personal data when it is stored or disclosed outside of the UK or the EU. If personal data is stored in the US important safeguards must be observed. This includes undertaking a transfer risk assessment and the ensuring that either the UK addendum which uses the existing EU standard contractual clauses to protect the data or the UK International data transfer agreement are in force.

Disposing of Data

The Trust is committed to keeping data for the minimum time necessary to fulfil its purpose. Full details of data retention can be found in the Retention Policy and Schedule.

Employee Data - the Trust will keep employment history data and health data for seven years. Data will be removed a minimum of six years after their employment with the Trust has finished, in order to meet data needs for pensions, taxation, potential or current disputes, or job references.

Health and Safety Data – the Trust will keep health and safety records of accidents that happen for three years after the date of accident, for six years after their employment with the Trust has finished.

Paper based records shall be disposed of in a confidential waste sack, confidential waste bin, or shredded. Electronic records will be deleted through the decommissioning of equipment by the IT department and digital records shall be deleted from databases at source.

Disposing of IT Equipment

Even if you think you've deleted data from your computer it's likely remaining somewhere in some form, so disposing of IT equipment securely is essential. You must contact the Chief Executive Officer to have IT equipment removed and disposed.

Email Security

Your email address is individually assigned to you and should not be shared with others. In your absence or for specific investigation purposes only emails may be accessed by authorised individuals. You should take the following steps to ensure the security of your emails.

- Consider whether the content of the email should be encrypted or password protected. If sending a spreadsheet containing personal data this must be password protected. The password should be delivered using an alternative method of communication e.g. Telephone or SMS.

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

- Never click on a link or share any information with anyone that you don't recognise - if in doubt check with the Information Security and Governance team or an individual with sufficient technological expertise.

IT Systems

Colleagues must undertake appropriate training to ensure sufficient security awareness and must make best attempts to protect their identity by using a strong password. Account passwords and usernames should not be shared without authorisation from the Directors.

Remote Working

Where a collleague works remotely from the premises, they shall ensure the adequate protection of the data to which they have access. This includes:

- keeping confidential and secure their access details (user name, password etc)
- protecting information from access by third parties (eg family, friends etc)
- password protecting documents, laptops, memory storage devices etc
- immediately reporting any breach or suspected breach of this policy to dpo@bikeabilitytrust.org

Confidentiality

When working for the Trust, colleagues will often need to have access to confidential information which may include, for example:

- information about individuals who are members or otherwise involved in Trust activities

- information about the internal business of the Trust
- information about others working for the Trust.

The Trust is committed to keeping this information confidential, in order to protect people and the Trust itself. 'Confidential' means that all access to information must be on a "need to know" and properly authorised basis. Employees must use only the information they have been authorised to use, and for purposes that have been authorised.

Colleagues must assume information is confidential unless they know it is intended by the Trust to be made public. Colleagues must also not disclose confidential information to unauthorised people or cause a breach of security. In particular colleagues must:

- not compromise or seek to evade security measures (including computer passwords)
- be particularly careful when sending information to other agencies and organisations
- not gossip about confidential information, with colleagues or people outside the Trust
- not disclose information — especially over the telephone or electronically — unless they are sure of who they are disclosing it to, and that they are authorised to have it.

If in doubt about whether to disclose information or not, colleagues should not guess and should withhold the information while they check with the Directors whether the disclosure is appropriate and liaise with the Chief Executive Officer for advice on the method of disclosure. In accordance with employment contract terms and conditions, employees' confidentiality obligations continue to apply indefinitely after they have stopped working for the Trust.

Record Keeping

When a new employee joins, a personnel file for the storage of records relating to them is set up then scanned electronically. Employees' records may contain documents such as:

- personal details such as name, address, telephone number(s), email address, date of birth, marital status, emergency contacts, employment/contract dates, rates of pay, bank account details, entitlements, absence records (sickness, holiday, parental leave etc), national insurance number, health questionnaires, occupational health reports, TU membership etc
- job description
- performance review (appraisal)
- assessment records and observations, including test results
- qualifications including copies of any certificates
- training and development plans and objectives
- continuous professional development (CPD / CPC) records*
- training and development activities completed, including evaluation forms
- references, authorisation checks such as DBS, right to work in the UK etc.

*The Trust may store records of employees' CPD but is not responsible for their CPD record keeping requirements, as determined by professional bodies.

Data use

Schedule 2 of the DPA lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed.

Personal data is at the greatest risk of loss, corruption or theft when it is accessed and used:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally - in particular it should never be sent by email as this form of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside the European Economic Area
- Employees should not save copies of personal data to their own computers, and should only access and update the secure central copy of any data.

Data accuracy

The law requires the Trust to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to make reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in as few places as necessary, and employees should not create any unnecessary additional data sets
- Employees should take every opportunity to ensure data is updated, for instance by confirming a instructor's details when they call
- The Trust will make it easy for data subjects to update the information the Trust holds about them, for instance via the instructor registration website portal
- Data should be updated as inaccuracies are discovered, for instance if an instructor can no longer be reached on their stored telephone number it should be removed from the database
- Should the Trust engage in direct marketing, it is the Marketing Director's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by the Bikeability Trust are entitled to:

- Ask what information the Bikeability Trust holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the Trust is meeting its data protection obligations.

If an individual contacts the Trust requesting this information, this is called a subject access request. It is the Trust's preference that subject access requests from individuals should be made by email, addressed to the Chief Executive Officer, the data controller for the Trust although individuals may make such request in any way that might be appropriate to them. The data controller can supply a

standard request form, although individuals do not have to use this. Generally, there is no charge for such a request. The data controller will aim to provide the relevant data within one month although this can be extended to a maximum of three months. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Bikeability Trust may disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board of Trustees and from the Trust's legal advisers where necessary.

Providing information

The Bikeability Trust aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights.

To these ends, the Bikeability Trust has a privacy statement setting out how data relating to the individuals is used by the Trust. This statement may be found in the Trust's registration record filed on the Information Commissioners Office website.

The Bikeability Trust

Document control	
File name / Version	14 Data protection policy v3
Approved by (name)	Alison Hill
Date	22nd August 2019
Date of approval by the Board	22nd August 2019
Last review date	23 January 2023
Date of next review	January 2024
Provenance	http://www.techdonut.co.uk/staff-and-it-training/your-it-policies/sample-data-protection-policy-template ACEVO Best practice templates