DATA PROTECTION POLICY

Introduction

DiversiTech International needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

For personal data and shared data refer to appendix 1

Why this policy exists

This data protection policy ensures DiversiTech International:

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

Data Protection Law

The Data Protection Act 1998 describes how organisations including DiversiTech International must collect, handle and store personal information.

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 Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Policy Scope

This policy applies to:

- The main site of DiversiTech International.
- All sites of DiversiTech International.
- All staff and volunteers of DiversiTech International.
- All contractors, suppliers and other people working on behalf of DiversiTech International.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Plus any other information relating to individuals.

Data Protection Risks

This policy helps to protect DiversiTech International from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Everyone who works for or with DiversiTech International has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Managing Director** is ultimately responsible for ensuring that DiversiTech International meets its legal obligations.

The **Managing Director** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The **Financial Controller** is responsible for:

- The data of all staff and or volunteers.
- This may be in the form of salaries, pensions etc.
- Staff contracts.
- Staff leaving DiversiTech International, the financial data will be held for at least 3 years as HMRC may request to see this information during this time.

The **Operations Manager** is responsible for:

- Keeping the Directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data DiversiTech International holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used 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 company is considering using to store or process data. For instance, cloud computing services.

Staff Joining DiversiTech International

- DiversiTech International will explain at the time of the induction the organisations which DiversiTech International will be sharing data with. For personal data and shared data refer to appendix 1

Staff leaving DiversiTech International

- DiversiTech International will hold personal information of employees, including contact details, appraisals and reviews and be kept for at least 5 years.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **DiversiTech International will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from the Operations Manager if they are unsure about any aspect of data protection.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Operations Manager.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Managers must store all data on their own individual Z Drive which they hold regarding their staff members.
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.

- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Use

Personal data is of no value to DiversiTech International unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

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**. The Operations Manager can explain how to send data to authorised external contacts.

Personal data should **never be transferred outside of the European Economic Area**.

Employees should not save copies of personal data to their own computers.

Always access and update the central copy of any data.

Data accuracy

The law requires DiversiTech International to take reasonable steps to ensure data is kept accurate and up to date.

*Communicate to current staff what data is held. Speak to your Manager.

Data storage

The more important it is that the personal data is accurate, the greater the effort DiversiTech International should put into ensuring it is stored correctly.

- It is the responsibility of all employees who work with data to take 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**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- DiversiTech International will make it **easy for data subjects to update the information** DiversiTech International holds about them. For instance, via the company website.
- Data should be **updated as soon as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is The Managing 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 DiversiTech International are entitled to:

- Ask **what information** the company 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 company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Operations Manager at KDraycott@diversitech.com. The Operations Manager can supply a standard request form, although individuals do not have to use this.

The Operations Manager will aim to provide the relevant data within 14 days.

The Operations Manager 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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, DiversiTech International will disclose requested data. However, the Operations Manager will ensure the request is legitimate, seeking assistance from the Director's and from the company's legal advisers where necessary.

Providing information

DiversiTech International aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

Assessor Name	John Lyle	**Job Title**	Quality / Operations Coordinator	**Date**	22 February 2023
Person to action points	Dave Bass	**Job Title**	Managing Director	**Review Date**	21 February 2024

SIGNED

Dave Bass

Managing Director

22 February 2023

Appendix 1

Data DiversiTech International Holds

DiversiTech International Staff Information Forms - Bank details of employees, National Insurance number, employee home address, Finance Department (**shared with FMP Global – Payroll Bureau**).

Pension Companies – personal data – Aviva, Legal and General, Mattioli Woods, Nest and Standard Life

Medical Insurance Provider held by the Finance Department – **(shared AXA PP Healthcare).**

Details of the next of kin – kept in Finance Department in locked cabinet.

Employee contracts – kept in locked cabinet by the Managing Director.

Driving Licenses and passports -kept on personal Z Drive by the Operations Manager