

Data Protection Policy

Microbee Group Ltd (hereafter “Microbee” or “the company”, comprising of Microbee Ltd, Microbee Bird Control Ltd and Microbee Tree Management Ltd) needs to gather and use certain information about individuals.

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

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

This data protection policy ensures that Microbee:

- 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.

The Data Protection Act 2018 describes how organisations – including Microbee – 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 2018 is underpinned by eight important principles. These say that personal data must:

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

People Risks and Responsibilities

This policy applies to the head office of Microbee, all staff and all contractors, suppliers and other people working on behalf of the company. 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;
- and any other information relating to individuals.

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

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

Everyone who works for or with Microbee has some responsibility for ensuring data is collected, stored and handled appropriately. Every person that handles personal data must ensure it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **directors** are ultimately responsible for ensuring that Microbee meets its legal obligations. They must:
 - Be aware of data protection responsibilities, risks and issues;
 - review all data protection procedures and related policies, in line with an agreed schedule;
 - arrange data protection training and advice for the people covered by this policy;
 - handle data protection questions from staff and anyone else covered by this policy;
 - deal with requests from individuals to see the data that Microbee holds about them (also known as 'subject access requests');
 - check and approve any contracts or agreements with third parties that may handle the company's sensitive data.
- **IT systems:**
 - ensure all systems, services and equipment used for storing data meet acceptable security standards;
 - perform regular checks and scans to ensure security hardware and software is functioning properly;
 - evaluate any third-party services that the company is considering using to store or process data, e.g. cloud computing services.
- **Marketing:**
 - approve any data protection statements attached to communications such as emails and letters;
 - address any data protection queries from journalists or media outlets like newspapers;
 - where necessary, work with other staff to ensure marketing initiatives abide by data protection principles.

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. Staff should only pass on data to another Microbee employee securely and responsibly, and only when they need it for their work.
- Microbee 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 should 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 it is no longer required, it should be deleted and disposed of.
 - Direct customer contact details (e.g. telephone number, email address, but not site address) should be deleted if it found to be no longer accurate or after 1 year has passed since the last time the customer was contacted.
 - Customer card details (as used in WorldPay card machine payments) should not be noted outside of a transaction literally being made there and then with a customer, and all copies of it should be handed over afterwards to the Finance Director, so it can be disposed of securely.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data protection officer.

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:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (such as CDs or DVDs), 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 approved cloud computing services (e.g. OneDrive, GorillaDesk).
- 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.
 - Photographs and video footage of customer property should be deleted from a technician's device after being forwarded to the office and after no more than 1 month after the end of the treatment.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no use to Microbee 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 IT manager can explain how to send data to authorised external contacts.
 - Microbee almost never sends out customer data, except when requested in very unusual circumstances (q.v. 'Disclosing Data for Other Reasons' below).
- 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.
 - Only the Document Control officer should be editing controlled documents, and all other staff should interact with a signed-off PDF copy (q.v. the company's Controlled Documents procedure).

Data Accuracy

The law requires Microbee to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that personal data is accurate, the greater the effort Microbee should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept 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.
- Microbee will make it easy for data subjects to update the information that the company holds about them (e.g. via the company website).
- Data should be updated as inaccuracies are discovered (e.g. if a customer can no longer be reached on their stored telephone number, it should be removed from the database).
- It is the marketing manager'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 Microbee 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 data protection officer at **info@microbee.co.uk**.

Individuals will be charged £10 per subject access request. The data protection officer will aim to provide the relevant data within 14 days.

The directors 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, Microbee will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the directors and from the company's legal advisers where necessary.

Providing Information


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

- how their data is being used;
- how to exercise their rights.



To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This privacy statement is available upon request.

This is the current copy of this policy.

Date:	5 th May 2020
Signed:	
Position:	Director
Review by:	May 2021 (or as necessary)