BROMLEY EDUCATION
be. be inspired

GDPR / Data Protection Policy – May 2018

1. Context and overview

Key details

- Policy prepared by: Matthew Bromley, Company Director
- Approved by board / management on: 18/05/2018
- Policy became operational on: 18/05/2018
- Next review date: 18/05/2019

Introduction

Autus Group Ltd/Bromley Education 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.

Why this policy exists

This data protection policy ensures Autus Group Ltd/Bromley Education:

- Complies with data protection law and follow 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 Autus Group Ltd/Bromley Education — 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:

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. 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

2. People, risks and responsibilities

Policy scope
This policy applies to:

- The head office of Autus Group Ltd/Bromley Education
- All staff of Autus Group Ltd/Bromley Education
- All contractors, suppliers and other people working on behalf of Autus Group Ltd/Bromley Education

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 Autus Group Ltd/Bromley Education 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.

Responsibilities

Everyone who works for or with Autus Group Ltd/Bromley Education has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team member 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 **company director/person of significant control** is ultimately responsible for ensuring that Autus Group Ltd/Bromley Education meets its legal obligations.

- **The Company Director,** is responsible for:

    - 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 Autus Group Ltd/Bromley Education 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.

- **The Company Director**, is also responsible for:

    - 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.

- **The Company 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.

3. 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.
- Autus Group Ltd/Bromley Education **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 company director if they are unsure about any aspect of data protection.

4. Data storage

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

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** (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**.

5. Data use

Personal data is of no value to Autus Group Ltd/Bromley Education 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 company director 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.

6. Data accuracy

The law requires Autus Group Ltd/Bromley Education to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Autus Group Ltd/Bromley Education 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 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.
- Autus Group Ltd/Bromley Education will make it **easy for data subjects to update the information** Autus Group Ltd/Bromley Education holds about them.
- Data should be **updated 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 company director's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

7. Subject access requests

All individuals who are the subject of personal data held by Autus Group Ltd/Bromley Education 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 company director at admin@bromleyeducation.co.uk. The company director can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The company director will aim to provide the relevant data within 30 days.

The company director will always verify the identity of anyone making a subject access request before handing over any information.

8. 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, Autus Group Ltd/Bromley Education will disclose requested data. However, the company director will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

9. Providing information

Autus Group Ltd/Bromley Education 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

Appendix 1

Your data

What data do we collect from you?

We collect basic contact details from all clients including:

- Name
- Email address
- Website address
- Postal address
- Telephone number

Where do we store your data?

This information is stored in our secure company email servers and, in some cases, in secure cloud storage servers including Apple iCloud, Google Drive and Dropbox. All information stored in the cloud is password protected and accessible only by our employees who have all had GDPR training and have read our data protection policy. All cloud servers are based within the EEA.

How do we use your data?

We do not share any of your data with third parties. It is used solely for the purposes of fulfilling our contractual obligations with you, for example to allow us to provide consultancy services or training. We use your data to personalise our products and services for you, and to keep you informed of our work. We use your data to provide customer care.

How long do we store your data?

We endeavour to delete all personal data once it is no longer in use. However, some data is retained to enable us to provide a better service to you. We review all our data – including that stored on our email servers and in cloud-based services – at least once every 12 months and delete data pertaining to any client for whom we have not worked for more than 6 months. We also delete data for current clients if we deem that data to be out of date or no longer useful in performing our duties.

You can request a copy of your data or request its erasure at any point by emailing us admin@bromleyeducation.co.uk