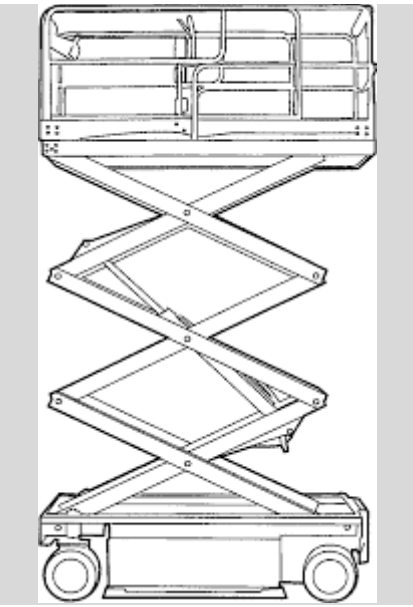
Galveston Grove
Oldfields Business Park
Fenton, Stoke-on-Trent
Staffordshire
ST4 3PE

Tel: 0800 0315175
Fax: 0844 770 9581
Mob: +44 (0) 787 552 9706
Email: jason@bellaaccess.com
Web: www.bellaaccess.com



Privacy Policy

Reference: Volume One
Initial Issue: February 2023
Review Date: February 2024

This Policy has been prepared by our retained health and safety advisors on behalf of Bella Access

BPA Services Limited
Quantum House
290 Leek Road
Stoke on Trent
Staffordshire
ST4 2BX

Tel: 01782 215664
Mob: 07539 153876

Email: g.howson@bpa-services.info

Web: www.bpa-services.com

Date Compiled: February 2023

Created By: Gemma Howson (BPA)
Of: BPA Services Limited

Revision	Date	Details
Prelim	**February 2023**	Creation
Version 2		
Version 3		
Version 4		
Version 5		
Version 6		
Version 7		
Version 8		
Version 9		

Policy Statement

This statement sets out Bella Access policy 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 under the Data Protection Act 2018, you have the right to find out what information Bella Access stores about you, including how your personal data must be collected, handled and stored to comply with the law. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

Bella Access will adhere to the company's data protection standards by adhering to the following:

- ✓ 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

Jason Dalmas
Managing Director

Bella Access
February 2023

Data Protection Law

The Data Protection Act 2018 describes how organisations including Bella Access must collect, handle and store personal information.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

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

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

People, Risk and Responsibilities

Policy Scope

This policy applies to:

- The office of Bella Access
- All staff of Bella Access
- All contractors, suppliers and other people working on behalf of Bella Access

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 2018. This can include (this may vary according to your relationship with us):

- Name;
- Date of birth;
- Gender;
- Address;
- Email address;
- Telephone number;
- Business name;
- Job title;
- Profession;
- National Insurance Number;
- Payment information;
- Information about your preferences and interests;
- Identification Documents;
- Criminal convictions;
- Occasionally we may receive information about you from other sources (such as credit reference agencies) which we will add to the information which we already hold about you in order to help us provide services.

Data Protection Risks

This policy helps to protect Bella Access 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 Bella Access 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 board of directors is ultimately responsible for ensuring that Bella Access meets its legal obligations.
- Bella Access has assessed that due to its small size and limited risk does not require a data protection officer, it is the responsibility of the directors to keep 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 Bella Access 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 Director, is 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.

General Manager, 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.

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.
- Bella Access 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 their line manager 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 Directors. 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, DVD and memory stick), 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 service.
- 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.
- Sensitive data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- 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 Bella Access 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. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Software 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 Bella Access 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 Bella Access 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.
- Bella Access will make it easy for data subjects to update the information Bella Access holds about them. As this is limited HR data this can be accessed by contacting
- Data should be updated as inaccuracies are discovered. For instance, if a staff member changes address.

Subject Access Requests

All individuals who are the subject of personal data held by Bella Access 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 Director who will aim to provide the relevant data within 14 days.

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

Proving Information

Bella Access 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

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

Jason Dalmas
Managing Director
Bella Access
February 2023