Data Protection Policy – GDPR

Date of Publication	**24th May 2018**
Date of Review	**24th May 2020**
Staff Member Responsible	**CEO**
Policy Creator	**CEO**
ICO Registration Number	**Z2373303**

Introduction

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) in the course of its work needs to gather and use certain information about individuals.

These can include members, consumers, 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 BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) :

• Complies with data protection law

• Protects the rights of staff, consumers 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 and The General Data Protection Regulation (GDPR) describe how organisations, including, BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) must collect, handle, use 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

---

Policy Scope

This policy applies to all staff of BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID). Any breach of this policy or of the Regulation itself will be considered an offence and the organisation's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) who have access to personal information, will be expected to read and comply with this policy. It is expected that any contracts signed with external bodies will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

Responsibilities

Everyone who works for or with BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone 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 is ultimately responsible for ensuring that BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) meets its legal obligations.

The CEO is the Data Protection Officer, and responsible for:

- Understanding data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Ensuring that the notification of BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) is kept accurate. Details of the notification of BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) can be found on the Office of the Information Commissioner's website. Our data registration number is: Z2373303.
- Arranging data protection training and advice for staff 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 BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) 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.
- 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 IT working on behalf of BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) 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.

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.

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) 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 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 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 (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 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

• When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

• Data must be encrypted before being transferred electronically. The DPO 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 BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) to take reasonable steps to ensure data is kept accurate and up to date.

• Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

• BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) will make it easy for data subjects to update the information it holds about them. For instance, via update subscription preferences on our email newsletters.

• Data should be updated as inaccuracies are discovered.

Cookies

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. By continuing to browse the site, you are agreeing to our use of cookies.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

If you do not agree to our use of cookies you can either stop using our website or block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

We use the following cookies:

· ***Strictly necessary cookies.*** These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.

· ***Analytical/performance cookies*****.** They allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.

· ***Functionality cookies.*** These are used to recognise you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).

· ***Targeting cookies.*** These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose.

The cookies that our website may use include:

Cookie	**Type**	**Purpose**	**More information**

Google Analytics	ANALYTICAL, PERFORMANCE	We use this to understand how the site is being used in order to improve the user experience. User data is all anonymous.	More information on how Google Analytics and privacy through google can be found, here.

Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.

Subject Access Requests

All individuals who are the subject of personal data held by BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) are entitled to;

• Ask what information the organisation 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 BSE DMO Limited 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 admin@ourburystedmunds.com and clearly marked Subject Access Request. The data protection officer will supply a standard request form.

The data protection officer will aim to provide the relevant data within seven days.

The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

In certain circumstances, The Data Protection Act (DPA) and The General Data Protection Regulation (GDPR) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Data Protection Officer will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from legal advisers where necessary.

Data Processing

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) aims to ensure that individuals are aware that their data is being processed, and that they understand:

- What data we hold
- How the data is being used
- How to exercise their rights

Data we hold

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID)

aims to ensure that data captured is limited to only what is essential to fulfil the requirements.

Data that BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) collect and hold includes, but is not limited to:

- First and Surname
- Date of Birth
- Email address
- Address including postcode
- Phone and mobile number
- Social identifiers
- Preference data – provided by you at the point of sign up
- Cookie and behavioural data – based on web and email activity
- Marketing opt-in data
- Email communications responses
- History – full audit trail of data usage for compliance requirements

If we hold data, or are asked to process data for, a child under 13, we will hold additional data, including but not limited to:

- Parent or guardian name and contact information
- Parental or guardian consent for marketing communications

We also collect information about how you use our website and mobile apps to improve SEO, PPC, online advertising, email marketing, web analytics or other digital services.

How we use your data

- Communication via email, post or SMS where we have valid opt in consent, for example updates on events and promotions
- Promotion of BSE DMO Limited and our products and services
- Profiling to improve our communication
- Research and statistical analysis to inform the DMO strategy and update members.

Your data will be shared with approved third parties in order to provide these services. For an up-to-date list of these third parties, please email admin@ourburystedmunds.com

Consent

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) values your privacy and will only communicate with you via email where we have valid opt in consent, gathered at the point of data collection.

All email communications include an unsubscribe link, so you can be removed from our communications at any time.

Alternatively, you can email admin@ourburystedmunds.com

How to exercise your rights with regard to processing

All individuals have the right to be removed from or restrict processing of their data by BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID). To exercise this right, send an email, addressed to the data protection officer at admin@ourburystedmunds.comThe data protection officer will supply a standard request form.

Data Breach Policy

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) understands that compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) is obliged under Data Protection legislation to have in place a procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definitions / Types of breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the information assets and / or reputation BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) of

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of PC, USB stick, mobile phone, or paper record)
- equipment theft or failure
- system failure
- unauthorised use of, access to or modification of data or information systems
- attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- unauthorised disclosure of sensitive / confidential data
- website defacement
- hacking attack
- unforeseen circumstances such as a fire or flood
- human error
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

Any individual who accesses, uses or manages information of BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (at info@burystedmundsandbeyond.co.uk) clearly marked 'Data Breach'.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process.

All staff should be aware that any breach of Data Protection legislation may result in the company's Disciplinary Procedures being instigated.

Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)
- whether the data could be put to any illegal or inappropriate use
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach.

Notification

The LIO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office (ICO) will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)

- whether notification would help prevent the unauthorised or unlawful use of personal data
- whether there are any legal / contractual notification requirements
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact BSE BID CO Limited and BSE BID CO (Events) Ltd (Our Bury St Edmunds BID) for further information or to ask questions on what has occurred.

The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The LIO and or the DPO will consider whether a press release should be prepared and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

<u>Evaluation and response</u>

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored
- where the biggest risks lie including identifying potential weak points within existing security measures
- whether methods of transmission are secure; sharing minimum amount of data necessary
- staff awareness
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security
- If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Board.

The Data Breach Policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Procedure for review

This Data Protection Policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The Data Protection Officer at admin@ourburystedmunds.com

This policy was last updated in May 2018.
