Data Protection Policy

Context and overview

Key Details

- Policy prepared by: Andrew Ralph
- Next review date: 01/04/19

Introduction

Bentley Photographic 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. These also include names for students to allow us to create named group photographs and student ID cards.

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

Why this policy exists

This data protection policy ensures Bentley Photographic:

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

Data protection law

The General Data Protection Regulation 2018 describes how organisations – including Bentley Photographic – must collect, handle and store personal information.

These rules apply regardless of wether 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 General Data Protection Regulation 2018 is underpinned by six important principles. These say that data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that in incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

People, risks and responsibilities

Policy scope

This policy applies to

- The head office of Bentley Photographic
- All branches of Bentley Photographic
- All staff and volunteers of Bentley Photographic
- All contractors, suppliers and other people working on behalf of Bentley Photographic

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018. This can include:

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

Data protection risks

This policy helps to protect Bentley Photographic 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 Bentley Photographic 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 Bentley Photographic meets its legal obligations.
- The **data protection officer, Andrew Ralph,** is responsible for:
    - Keeping the board 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 Bentley Photographic 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.
    - 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 manager, Chris Hampton,** 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 **office manager,** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.

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
- **Bentley Photographic 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 r**egularly 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 IT manager or data controller.

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
- 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 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
- 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 Bentley Photographic 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
- 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 Bentley Photographic 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 Bentley Photographic 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.
- Bentley Photographic will make it easy for data subjects to update the information Bentley Photographic holds about them. For instance, via the company website.
- 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.
- Marketing databases should be checked against industry suppression files every six months.

Online Orders

Bentley Photographic uses on online ordering system provided by Xanda Ltd. The website has a SHA-256 SSL certificate. All payments are processed remotely. No credit card information information is processed or stored by Bentley Photographic.

Orders that are to be posted to home addresses are not sent with any personal data other than the name and address to which the order is to be delivered.

Subject access requests

All individuals who are the subject of personal data held by Bentley Photographic 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 controller at info@bentleyphoto.com. The data controller can supply a standard request form, although individuals do not have to use this.

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

The data controller 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 General Data Protection Regulations allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Bentley Photographic 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.

Providing information

Bentley Photographic 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