Data Protection Policy

Reference:	Data Protection Policy
Date Approved:	9th May 2018
Approved by:	Adam Simmons
Implementation Date:	9th May 2018
Version:	Issue 1
Supersedes:	N/A
Target Audience:	Staff, Subcontractors, Suppliers
Review Date:	1 year from publication

1. Introduction

Barons Group Ltd 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.

Such information includes Personal Data, which is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. This data protection policy ensures Barons:

- 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.

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 law. This policy sets forth the expected behaviours of Barons employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Barons Contact (i.e. the Data Subject). This policy helps to protect Barons 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.

Barons Group Ltd leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Barons Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved on behalf of the Barons Group Limited by:

Adam Simmons
Director

2. Scope

This policy applies to:

- The head office of Barons;
- All branches and site offices of Barons;
- All staff and volunteers of Barons;
- All contractors, suppliers and other people working on behalf of Barons;

It applies to all data that the company holds relating to identifiable individuals, even if that information is available within the public domain. This can include:

- Names of individuals
- Postal addresses
- Email addresses (personal or business)
- Telephone numbers
- …plus any other information relating to individuals

This policy applies where a Data Subject's Personal Data is processed:

- In the context of the business activities of Barons.
- For the provision or offer of goods or services to individuals by Barons.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3. Definitions

Employee	An individual who works part-time or full-time for Barons under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and agency staff.
Third Party	An external organisation with which Barons conducts business and is also authorised to, under the direct authority of Barons, Process the Personal Data of Barons Contacts.
Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Contact	Any past, current or prospective Barons customer or supplier.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	The identified or Identifiable Natural Person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, which may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Encryption	Converting information or data into code, to prevent unauthorised access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. Responsibilities

Everyone who works for or with **Barons** 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. Importantly, everyone has a responsibility to notify of a suspected data breach. However, these people have key areas of responsibility:

- The **Directors** are ultimately responsible for:
    - Ensuring that **Barons** meets its legal obligations.
    - Ensure that all Barons employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.
    - All Barons employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training.

- The **Data Protection Administrator, Heather Quiroga,** 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 Barons holds about them (also called 'subject access requests').
    - Regular data audits to manage and mitigate risks to inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

- The **Director, Adam Simmons,** 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.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

5. Data Protection Principles

Barons has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1: Lawfulness, Fairness and Transparency:** Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
- **Principle 2: Purpose Limitation:** Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means that Barons will limit the Processing of Personal Data to only what is necessary to meet the specified purpose.
- **Principle 3: Data Minimisation:** Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means Barons must not store any Personal Data beyond what is strictly required.
- **Principle 4: Accuracy:** Personal Data shall be accurate and, kept up to date. This means Barons must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
- **Principle 5: Storage Limitation:** Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed.
- **Principle 6: Integrity & Confidentiality:** Personal Data shall be 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. Barons must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

6. Policy

6.1. Data Processing

6.1.1. Basis for Data Processing

Barons uses the Personal Data of its Contacts & Employees for the following broad purposes:

- The general running and business administration of Barons.
- To provide services to Barons customers.
- The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Barons to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Barons would then provide their details to Third Parties for marketing purposes.

All employees and departments will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Barons will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

In any circumstance where Consent has not been gained for the specific Processing in question, Barons will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

6.1.2. Sensitive Personal Data

Barons will only Process Special Categories of Data (also known as Sensitive Personal Data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Data Protection Administrator and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, Barons will adopt additional protection measures.

6.1.3. Data Subject Consent

Barons will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Barons is committed to seeking such Consent.

The Data Protection Administrator, in cooperation with the Board, and other relevant business representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

6.1.4. Digital Marketing

As a general rule Barons will not send promotional or direct marketing material to a Barons Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any department wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Data Protection Administrator.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

6.2. Protecting data integrity & quality

6.2.1. 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.
- **Barons 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 administrator if they are unsure about any aspect of data protection.

6.2.2. 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 Administrator or Chairman.

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.
- 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.

6.2.3. Data use

Personal data is of no value to Barons 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.
- Personal data should **never be transferred outside of the EU** without checking the receiving organisation has adequate safeguards in place.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

6.2.4. Data Quality

The law requires Barons to take reasonable steps to ensure data is kept accurate and up to date. Barons will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject. 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.
- 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.

6.2.5. Data Retention

To ensure fair Processing, Personal Data will not be retained by Barons for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. The length of time for which Barons needs to retain Personal Data is set out in the Barons' Personal Data Retention Schedule'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

6.2.6. Breach Reporting

A data breach is "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data". **Failure to notify a breach when required to do so can result in a fine up to €10m or 2% of annual turnover.** There are tight timescales for reporting a breach to the relevant supervisory authority – this must be done within 72 hours of Barons becoming aware of the breach.

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must **immediately** notify the Data Protection Administrator providing a description of what occurred. The Data Protection Administrator will investigate all reported incidents to confirm whether a Personal Data Breach has occurred.

If a Personal Data Breach is confirmed, the Data Protection Administrator will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. It is mandatory to report a Personal Data Breach under the GDPR if it's likely to result in a risk to people's rights and freedoms.

Notification of the incident can me made via e-mail heather @barons-group.org

6.3. Requests, Disclosures and Third-Party Transfers

6.3.1. Data Subject Requests

The Data Protection Administrator, in conjunction with the Board, will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing or to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, Barons will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. Data Subjects are entitled to obtain, based upon a request made in writing to the Data Protection Administrator and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Data Protection Administrator, who will log each request. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Barons to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Barons cannot respond fully to the request within 30 days, the Data Protection Administrator shall provide the following to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. if the request is excessive in nature).

- The contact information of the Barons individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

6.3.2. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

Under these circumstances, Barons 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.

6.3.3. Transfers to Third Parties

Barons will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Barons will enter into, an appropriate agreement clarifying each party's responsibilities in respect to the Personal Data transferred.

The agreement will require the Third Party to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Barons instructions. In addition, the agreement will require the Third Party to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

When considering outsourcing services to a Third Party (including Cloud Computing services), Barons will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

7. Policy Maintenance

7.1. Enquiries

All enquiries about this policy, including requests for exceptions or changes should be directed to the Data Protection Administrator via e-mail heather @barons-group.org

7.2. Publication

This policy shall be available to all Barons Employees through the Master Documents folder