Data Protection Policy

A) INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy applies to the processing of personal data in manual and electronic records, and covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of existing and former employees, job applicants, apprentices, volunteers, placement students, learners and self-employed contractors. These are referred to in this policy as relevant individuals.

B) DEFINITIONS

BAJ – British Academy of Jewellery, 81-84 Chalk Farm Road, Camden, London, NW1 8AR

BAJ Personnel – Any BAJ employee, worker or contractor who accesses any BAJ Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of BAJ.

Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data of which BAJ is the Controller include employee details or information BAJ collects which relates to students. BAJ will be viewed as a Controller of Personal Data if it decides what Personal Data it is going to collect and how it will use it.

A common misconception is that individuals within organizations are the Controllers. This is not the case; it is the organization itself which is the Controller.

Data processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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 Laws – The General Data Protection Regulation (GDPR) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – Our Data Protection Officer is Ori Lamm, who can be contacted at: ori.lamm@baj.ac.uk

EEA – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Individuals – Living individuals who can be identified, directly or indirectly, from information that BAJ has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, job applicants, students, contractors, visitors and potential students.

Personal Data – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data, exam results and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

Personal Data will only be shared with parents or next of kin if the individual has given us permission to do so or has processed a written request. We will not give personal data to anyone without the written permission or request from the individual. This includes issues such as giving student performance information to potential employers.

Processor – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business, cloud arrangements, and mail fulfillment services.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

Criminal offence data - Data which relates to an individual's criminal convictions and offences.

C) BAJ PERSONNEL'S OBLIGATIONS AND RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

All BAJ Personnel must comply with this policy.

BAJ Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

BAJ Personnel must not release or disclose any Personal Data outside BAJ - or inside BAJ to BAJ Personnel not authorised to access the Personal Data - without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

BAJ Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other BAJ Personnel who are not authorised to see such Personal Data or by people outside BAJ.

D) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent.
b) data be collected for specific, explicit, and legitimate purposes.
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing.
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay.
e) data is not kept for longer than is necessary for its given purpose.
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
g) we will comply with the relevant GDPR procedures for international transferring of personal data.

E) LAWFUL BASES OF PROCESSING

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the individual's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

F) TRANSPARENCY OF PROCESSING – PRIVACY NOTICES

Where BAJ collects Personal Data directly from Individuals, BAJ will inform them about how it uses their Personal Data through a privacy notice. BAJ has created different privacy notices for employees, job applicants, contractors, and customers.

If BAJ changes how it uses Personal Data, BAJ may need to notify Individuals about the change. If BAJ Personnel therefore intend to change how they use Personal Data, please notify the Data Protection Officer who will decide whether the BAJ Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

G) DATA QUALITY

Data Protection Laws require that BAJ only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice, and as set out in BAJ record of how it uses Personal Data. BAJ is also required to ensure that the Personal Data it holds is accurate and kept up to date.

All BAJ Personnel who collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date, and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

All BAJ Personnel who obtain Personal Data from sources outside BAJ shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require BAJ Personnel to independently check the Personal Data obtained.

In order to maintain the quality of Personal Data, all BAJ Personnel who access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which BAJ must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

BAJ recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. BAJ has a Rights of Individuals Policy and a dedicated Rights of Individuals form which set out how BAJ responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

H) TYPES OF DATA HELD

We keep several categories of personal data on individuals in order to carry out effective and efficient processes. We keep this data in a file relating to each individual and we also hold the data within our computer systems.

Detailed information on the categories of personal data we hold and our processing activities is included in our different Privacy Notices.

I) INDIVIDUALS' RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate Subject Access Request Policy";
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate Rights of Individuals Policy.

BAJ will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with BAJ's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which BAJ Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

J) ACCESS TO DATA

As stated above, individuals have a right to access the personal data that we hold on them. To exercise this right, individuals should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

K) DATA DISCLOSURES

BAJ may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) any individual benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d) for Statutory Sick Pay purposes;
e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any employee insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

L) MARKETING AND CONSENT

BAJ will sometimes contact Individuals to send them marketing or to promote BAJ. Where BAJ carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR brought about a number of important changes for organisations that market to individuals, including providing more detail in their privacy notices (including for example whether profiling takes place), rules on obtaining consent are stricter and require an individual's "clear affirmative action".

BAJ also needs to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside Data Protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

Consent is central to electronic marketing, and the best practice is to provide an un-ticked opt-in box.

Alternatively, BAJ may be able to market using a “soft opt in” if the following conditions were met:

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- BAJ are marketing its own similar services;
- BAJ gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

M) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain BAJ’s commitment to protecting data in line with Data Protection Laws.

N) AUTOMATED DECISION MAKING AND PROFILING

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where BAJ makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects.

Profiling happens where BAJ automatically uses Personal Data to evaluate certain things about an Individual.

Any Automated Decision Making or Profiling which BAJ carries out can only be done once we are confident that it is complying with Data Protection Laws. If BAJ Personnel therefore wish to carry out any Automated Decision Making or Profiling they must inform the Data Protection Officer.

BAJ Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

BAJ currently does not carry out Automated Decision Making or Profiling in relation to individuals.

O) INTERNATIONAL DATA TRANSFERS

Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. This needs to be considered whenever BAJ appoints a supplier outside the EEA or whenever BAJ appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

So that BAJ can ensure it is compliant with Data Protection Laws, BAJ Personnel must not export Personal Data outside the EEA unless it has been approved by the Data Protection Officer.

P) DATA SECURITY

Employees are aware of their roles and responsibilities when their role involves the processing of data.

All employees are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them, and to ensure that screen locks are implemented on all PCs, laptops and tablets when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

All our employees are aware that a hard copy containing personal information should be kept in a locked filing cabinet, drawer, or safe.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to individuals should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created in or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow BAJ's rules on data security may be dealt with via the company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Q) REQUIREMENT TO NOTIFY BREACHES

Whilst BAJ takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and BAJ Personnel must comply with BAJ's Data Breach Notification Policy. Please see below examples of what can constitute a Personal Data breach, and familiarise yourself with these, as they contain important obligations which BAJ Personnel need to comply with in the event of Personal Data breaches.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of internal misuse.

There are three main types of Personal Data breach:

Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that BAJ Personnel are not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person.

Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key.

Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

R) TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the company of any potential lapses and breaches of the company's policies and procedures.

S) RECORDS

BAJ keeps records of its processing activities including the purpose for the processing and retention periods in its Data Records. These records will be kept up to date so that they reflect current processing activities.

Data Protection Laws require that BAJ does not keep Personal Data longer than is necessary for the purpose or purposes for which BAJ collected it.

BAJ has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by BAJ. BAJ securely shreds paper records and securely deletes electronic records of Personal Data at the end of those periods.

If BAJ Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the set retention period (for example because there is a requirement of law), or if BAJ Personnel have any questions about this Policy or BAJ's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

T) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Ori Lamm
ori.lamm@baj.ac.uk