The Salt Foundation Data Protection Policy June 2021

Table of Contents

1 Purpose

The Salt Foundation's (hereafter referred to as the Foundation) reputation and future growth are dependent on the way it manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the Foundation.

As an organisation we, together with our agents Shipley College, collect, use and store Personal Data about our employees, suppliers, site users, trustees, volunteers, and visitors. Personal information is collected to effectively carry out our everyday business functions and activities. In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law. the Foundation recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with its obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The Foundation has implemented this Data Protection Policy to ensure all its Trustees and employees are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

The Foundation employees will be directed to read this Policy when they start and may receive periodic revisions. This Policy does not form part of any employee's contract of employment and the Foundation reserves the right to change this Policy at any time. All Foundation employees and Trustees are obliged to comply with this Policy at all times.

The majority of the Foundation's data is held and managed by its agents, Shipley College. Therefore this policy mirrors that of Shipley College and reporting is via the College processes. Any variations to the College policy are in blue text. The Foundation is not required to register with the ICO and therefore does not have a Data Protection Officer. If you have any queries concerning this Policy, please contact DPO@shipley.ac.uk and one of the College team will respond.

2 Scope

This Policy (and the other policies and documents referred to in it) sets out the basis on which the Foundation will collect and use Personal Data either where the Foundation collects it directly from individuals, or where provided to the Foundation by third parties. It also sets out rules on how the Foundation handles uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

Employees Responsibilities:

- To comply with this Policy
- To ensure that you keep confidential all Personal Data that we collect, store, use and come into contact with during the performance of your duties
- To not release or disclose any Personal Data outside the Foundation or inside the Foundation to others not authorised to access the Personal Data; without specific authorisation from your manager or the Data Protection Officer; this includes disclosure verbally or in writing
- To take all steps to ensure there is no unauthorised access to Personal Data (this includes other employees who are not authorised to see such Personal Data as well as by people outside the Foundation.

3 Data Protection Principles

When using Personal Data, Data Protection Laws require that the Foundation complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

- kept for no longer than is necessary for the purposes for which it is being processed; and

- 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.

These principles are considered in more detail in the remainder of this Policy.

In addition to complying with the above requirements, the Foundation also has to demonstrate in writing that it complies with them. The Foundation has a number of policies and procedures in place, including this Policy and the Retention and Disposal Schedule in appendix 1 and the documentation referred to in it, to ensure that it can demonstrate its compliance.

4 Lawful Use Of Personal Data

In order to collect and/or use Personal Data lawfully the Foundation needs to be able to show that its use meets one of a number of legal grounds. Click here to see the detailed grounds.

In addition, when the Foundation collects and/or uses Special Categories of Personal Data, it has to show that one of a number of additional conditions is met. Click here to see the detailed additional conditions.

The Foundation has carefully assessed how it uses Personal Data and how it complies with its obligations. If the Foundation changes how it uses Personal Data, it needs to update this record and may also need to notify individuals about the change. If employees therefore intend to change how they use Personal Data at any point they must notify the Trustees who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

5 Transparent Processing – Privacy Notices

Where the Foundation collects Personal Data directly from individuals, it will inform them about how it uses their Personal Data. This is in a privacy notice. the Foundation has adopted the following privacy notices:

- Victoria Hall Client Privacy Notice
- Current and Prospective Employee Privacy Notice (see Shipley College version)
- Trustee Privacy Notice
- Non Employed Individuals Privacy Notice (see Shipley College version)
- Supplier Privacy Notice (see Shipley College version)

If the Foundation receives Personal Data about an individual from other sources, it will provide the individual with a privacy notice about how the Foundation will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

6 Data Quality – Ensuring The Use Of Accurate, Up To Date And Relevant Personal Data

Data Protection Laws require that the Foundation 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 (see above) and as set out in the Foundation's record of how it uses Personal Data. the Foundation is also required to ensure that the Personal Data it holds is accurate and kept up to date.

All employees who collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and 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.

In order to maintain the quality of Personal Data, all employees that access Personal Data shall ensure that they review 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. This does not require an independent check of the Personal Data obtained. Please note that this does not apply to Personal Data which the Foundation must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

The Foundation recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. Within this Policy, the rights of individuals are set out. 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 the information within this Policy.

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

The Foundation 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, the reasons for those retention periods and how it securely deletes Personal Data at the end of those periods. These are set out in the Data Retention schedule in Appendix 1.

If employees feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if employees have any questions about this Policy or the Foundation's Personal Data retention practices, they should contact dpo@shipley.ac.uk for guidance.

7 Data Security

The Foundation and its agent, Shipley College, has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The Foundation and its agent, Shipley College have in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

8 Data Breach

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 employees must comply with the Notification Procedure (appendix 3).

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 something someone internal does.

There are three main types of Personal Data breach which are as follows:

Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that an employee is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student or staff member, 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 ransomware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from backup, or loss of an encryption key; and

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

9 Appointing Contractors Who Access the Foundation's Personal Data

If the Foundation appoints a contractor (directly or via its agent Shipley College) who is a Processor of the Foundation's Personal Data, Data Protection Laws require that any such appointment would only be made after sufficient due diligence and where appropriate contracts are in place.

One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract where an organisation appoints a Processor must be in writing.

You are considered as having appointed a Processor where you engage someone to perform a service for you and, as part of it, they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller
- to not export Personal Data without the Controller's instruction
- to ensure staff are subject to confidentiality obligations
- to take appropriate security measures
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract
- to keep the Personal Data secure and assist the Controller to do so
- to assist with the notification of Data Breaches and Data Protection Impact Assessments
- to assist with subject access/individuals rights
- to delete/return all Personal Data as requested at the end of the contract
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law

In addition the contract should set out:

- The subject-matter and duration of the processing
- the nature and purpose of the processing
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller

10 Individuals' Rights

There is an expectation that the Foundation complies with its legal obligations to allow individuals to exercise their rights over their Personal Data. GDPR gives individuals more control about how their

data is collected and stored and used. Some existing rights of individuals have been expanded upon and some new rights have been introduced. the Foundation must have a procedure to handle these requests under GDPR.

Employees Responsibilities

If an employee receives a request from an individual to exercise any of the rights set out in this Policy, that member must:

- inform dpo@shipley.ac.uk as soon as possible and, in any event, within 24 hours of receiving the request;
- including, what the request consists of, who has sent the request and provide a copy of the request;
- not make any attempt to deal with, or respond to, the request without authorisation from the Foundation Data Protection Officer.

11 Right Of Access (Subject Access Requests)

Individuals have the right to ask the Foundation to confirm the Personal Data about them that it is holding, and to have copies of that Personal Data (commonly known as a Subject Access Request or SAR) along with the following information:

- the purposes for which the Foundation has their Personal Data
- the categories of Personal Data about them that the Foundation has
- the recipients or categories of recipients to whom their Personal Data has been or will be disclosed
- how long the Foundation will keep their Personal Data
- that they have the right to request that the Foundation corrects any inaccuracies in their Personal Data or deletes their Personal Data (in certain circumstances, please see below for further information); or restrict the uses the Foundation is making of their Personal Data (in certain circumstances, please see below for further information); or to object to the uses the Foundation is making of their Personal Data (in certain circumstances, please see below for further information)
- that they have the right to complain to the ICO if they are unhappy about how the Foundation has dealt with this request or in general about the way the Foundation is handling their Personal Data
- where the Personal Data was not collected from them, where the Foundation got it from
- the existence of automated decision-making, including profiling (if applicable).

The Foundation is not entitled to charge individuals for complying with this request. However, if the individual would like a further copy of the information requested, the Foundation can charge a reasonable fee based on its administrative costs of making the further copy.

There are no formality requirements to making a Subject Access Request and it does not have to refer to data protection law, or use the words Subject Access Request or SAR. The Foundation will monitor its incoming communications, including post, email, its website and social media pages to ensure that the Foundation can recognise a SAR when it receives it.

The Foundation is required to respond to a SAR within one month from the date it is received. If the SAR is complex or there are multiple requests at once, the Foundation may extend this period by two further months provided that it tells the individual who has made the SAR about the delay and the Foundation's reasons for the delay within the first month.

The Foundation Executive committee will reach a decision as to the complexity of the SAR and whether the Foundation is entitled to extend the deadline for responding.

12 Right to rectification

Individuals have the right to ask the Foundation to correct any Personal Data about them that it is holding that is incorrect. the Foundation is then obliged to correct that Personal Data within one month (or two months if the request is complex).

Where the individual tells the Foundation their Personal Data is incomplete, it is obliged to complete it if the individual requests Where the individual tells the Foundation their Personal Data is incomplete, it is obliged to complete it if the individual requests this. A supplementary statement may be added to the individual's personal file.

If the Foundation has disclosed the individual's inaccurate Personal Data to any third parties, it is required to tell the individual who those third parties are and to inform the third parties of the correction where the Foundation can.

When an individual asks the Foundation to correct their Personal Data, it is required to do so and to confirm this in writing to the individual within one month of the request.

13 Right to erasure (right to be forgotten)

Individuals have the right to ask the Foundation to delete the Personal Data it has about them in certain circumstances but this right is limited in scope and does not apply to every individual. The right to be forgotten applies when:

- the Personal Data is no longer necessary for the purpose for which it was collected;
- the individual withdraws consent and the Foundation has no other legal basis to use their Personal Data;
- the individual objects to the Foundation's processing and there is no overriding legitimate interest for continuing the processing;
- the Personal Data was unlawfully processed; and/or
- the Personal Data has to be erased to comply with a legal obligation.

If the Foundation has disclosed the individual's deleted Personal Data to any third parties, it is required to tell the individual who those third parties are and to inform the third parties to delete the Personal Data where possible.

When an individual asks the Foundation to delete their Personal Data, the Foundation is required to do so and to inform the individual in writing within one month of them making the request that this has been done.

14 Right to restrict processing

Individuals have the right to "block" or "suppress" the Foundation's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the Foundation to verify the accuracy of the Personal Data;
- the processing is unlawful and the individual opposes the deletion of the Personal Data and requests restriction instead;

- the Foundation no longer needs the Personal Data for the purposes it was collected, butis required by the individual to keep the Personal Data for the establishment, exercise or defence of legal claims;

- the individual has objected to the Foundation's legitimate interests, for a period enabling the Foundation to verify whether its legitimate interests override their interests.

If the Foundation has disclosed the individual's restricted Personal Data to any third parties, it is required to tell the individual who those third parties are and to inform the third parties about the restriction where the Foundation can.

When an individual asks the Foundation to restrict its processing of their Personal Data, it is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

15 Right to data portability

Individuals have the right to obtain from the Foundation a copy of their own Personal Data in a structured, commonly used and machine readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

The right to data portability only applies when:

- the individual provided the Foundation with the Personal Data;

- the processing the Foundation is carrying out is based on the individual's consent or is necessary for the performance of a contract; and

- the processing is carried out by automated means.

- This means that the right to data portability does not apply to Personal Data the Foundation is processing on another legal basis, such as its legitimate interests.

- the Foundation is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that it explains to the individual why it needs more time).

- The individual also has the right to ask the Foundation to transmit the Personal Data directly to another organisation if this is technically possible.

16 Right to object

Individuals have the right to object to the Foundation's processing of their Personal Data where:

- the Foundation's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;

- the Foundation is carrying out direct marketing to the individual; and/or

- the Foundation's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

- If an individual has grounds to object to the Foundation's legitimate interests, the Foundation must stop processing their Personal Data unless there are compelling legitimate grounds for the processing which override the interests of the individual, or where the processing is for the establishment, exercise or defence of legal claims.

- If an individual objects to direct marketing, the Foundation must stop processing their Personal Data for these purposes as soon as it receives the request. the Foundation cannot refuse their request for any reason and cannot charge them for complying with it.

- Before the end of one month from the date the Foundation gets the request, it must notify the individual in writing that it has complied or intends to comply with their objections or that it is not complying and the reasons why.

17 Rights in relation to automated decision making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:

- necessary for entering into or performing a contract between the Foundation and the individual;

- required or authorised by Data Protection Laws; or

- based on the individual's explicit consent.

Automated decision making happens where the Foundation makes a decision about an individual solely by automated means without any human involvement; and

Profiling happens where the Foundation automatically uses Personal Data to evaluate certain things about an individual.

Any Automated Decision Making or Profiling which the Foundation carries out can only be done once the Foundation is confident that it is complying with Data Protection Laws. If employees therefore wish to carry out any Automated Decision Making or Profiling they must inform dpo@shipley.ac.uk

18 Marketing And Consent

The Foundation will sometimes contact individuals to send them marketing or to promote the Foundation. Where the Foundation 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 will bring 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; and

- rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO likes consent to be used in a marketing context.

The Foundation ensures its awareness of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR applies 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.

The Foundation understands that consent is central to electronic marketing and follows, in the majority of its marketing activities, best practice by providing an un-ticked opt-in box. However, the Foundation may chose 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)

- the Foundation is marketing its own similar services; and
- the Foundation 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.

19 Data Protection Impact Assessments (DPIA)

The GDPR introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. All risk assessments will be carried out by the Foundation's agents, Shipley College using their own guidelines.

20 Transferring Personal Data To A Country Outside The EEA

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. It needs to be thought about whenever the Foundation or its agent, Shipley College, appoints a supplier outside the EEA or a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

So that the Foundation can ensure it is compliant with Data Protection Laws, employees must not export Personal Data unless it has been approved by the Trustees.

21 Monitoring and Reporting

The Policy will be monitored by the Trustees on a regular basis in line with the 2 yearly reviews of the Shipley College policy.

22 Links to other Policies & Procedures

This Policy reflects the Shipley College Data Protection policy and related policies and procedures.

Appendix 1 - Data Retention Schedule

The Foundation will follow the Shipley College Data Retention Schedule where relevant.

Appendix 2 - Definitions

The Salt Foundation– Victoria Road, Saltaire, BD18 3JS

Employees – Any Salt Foundation employee, including those employed by Shipley College as agents for the Foundation, worker or contractor who accesses any of the Foundation's Personal Data and will include employees, consultants, contractors, and temporary employees hired to work on behalf of the Foundation.

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 the Foundation is the Controller of include employee details or information the Foundation collects relating to students. The Foundation will be viewed as a Controller of Personal Data if it decides what Personal Data the Foundation is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case, it is the organisation itself which is the Controller.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) 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.

DPO@shipley.ac.uk – the Foundation is not required to have a dedicated Data Protection offices but any queries or breaches can be referred to the Shipley College DPO team by emailing DPO@shipley.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 the Foundation 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, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

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 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.

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 fulfilment 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.

Appendix 3 – Data Breach Notification Procedure

Please follow the procedure described in Appendix 3 the Shipley College Data Protection policy.