	DATA PROTECTION POLICY 21/23
Version:	FINAL
Author:	Data Protection Officer and DP Leads
Date Issued:	June 2021
Date Approved by SMT:	June 2021
Date Approved by Audit Committee:	June 2021
Date Approved by Corporation:	July 2021
Impact Assessment Completed	Yes
Date of Next Review:	May 2023

Quality Impact Assessment Form

The completion of the Equality Impact Assessment (EIA) will help us to ensure that our policies, procedures and practices do not discriminate or disadvantage people and also improve or promote equality.

In relation to: disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation.
1. Please explain if you identified any inequalities or possible discrimination in the policy, procedure or practice?
None identified
2. If identified, how have you changed the policy, procedure or practice to remove or mitigate the inequality or discrimination?
N/A
3. Any follow up actions required?
N/A

Table of Contents

1 Purpose

The College's 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 College.

As an organisation we collect, use and store Personal Data about our employees, suppliers~~,~~ learners, governors, parents, volunteers, visitors and other site users. 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 College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

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

College 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 College reserves the right to change this Policy at any time. All College employees are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, Ian Durham (DPO@shipley.ac.uk telephone 7253) who is responsible for ensuring the College's compliance with this Policy.

2 Scope

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College 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 College or inside the College 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 College employees who are not authorised to see such Personal Data as well as by people outside the College.

3 Data Protection Principles

When using Personal Data, Data Protection Laws require that the College 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 College also has to demonstrate in writing that it complies with them. The College 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 the College can demonstrate its compliance.

4 Lawful Use Of Personal Data

In order to collect and/or use Personal Data lawfully the College 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 College 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 College has carefully assessed how it uses Personal Data and how it complies with its obligations. If the College changes how it uses Personal Data, it needs to update this record and may also need to notify Individuals about the change. If College employees therefore intend to change how they use Personal Data at any point they must notify the College Data Protection Officer 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 College collects Personal Data directly from individuals, the College will inform them about how it uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices:

- Learner Privacy Notice
- Current and Prospective Employee Privacy Notice
- Governor Privacy Notice
- Non Employed Individuals Privacy Notice
- Supplier Privacy Notice

If the College receives Personal Data about an individual from other sources, it will provide the individual with a privacy notice about how the College 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 College 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 College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

All College 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 College 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 College Personnel to independently check the Personal Data obtained. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

The College 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 College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

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

If College 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 College employees have any questions about this Policy or the College's Personal Data retention practices, they should contact the College Data Protection Officer for guidance.

7 Data Security

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has 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

Whilst the College 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 College employees must comply with the College's Data Breach Notification Procedure (appendix 3). Employees must familiarise themselves with it as it contains important obligations which College employees 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 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 a College 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 College's Personal Data

If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts 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 College 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 what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that colleges plan how they will 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 the College Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request;
- tell the College Data Protection Officer what the request consists of, who has sent the request and provide the Data Protection Officer with a copy of the request;
- not make any attempt to deal with, or respond to, the request without authorisation from the College Data Protection Officer.

11 Right Of Access (Subject Access Requests)

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

The College 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 College 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 College will monitor its incoming communications, including post, email, its website and social media pages to ensure that the College can recognise a SAR when it receives it.

The College 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 College may extend this period by two further months provided that it tells the individual who has made the SAR about the delay and the College's reasons for the delay within the first month.

The Data Protection Officer will reach a decision as to the complexity of the SAR and whether the College is entitled to extend the deadline for responding.

12 Right to rectification

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

Where the individual tells the College their Personal Data is incomplete, the College is obliged to complete it if 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 College has disclosed the individual's inaccurate Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction where the College can.

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

13 Right to erasure (right to be forgotten)

Individuals have the right to ask the College to delete the Personal Data the College 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 College has no other legal basis to use their Personal Data;
- the individual objects to the College'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 College has disclosed the individual's deleted Personal Data to any third parties, the College 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 College to delete their Personal Data, the College 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 College's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the College 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 College no longer needs the Personal Data for the purposes it was collected, but the College is required by the individual to keep the Personal Data for the establishment, exercise or defence of legal claims;

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

If the College 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 College can.

When an individual asks the College 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 College 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 College with the Personal Data;

- the processing the College 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 College is processing on another legal basis, such as its legitimate interests.

- The College 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 the College explains to the individual why it needs more time).

- The individual also has the right to ask the College 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 College's processing of their Personal Data where:

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

- the College'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 College's legitimate interests, the College must stop processing their Personal Data unless the College has 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 College must stop processing their Personal Data for these purposes as soon as the College receives the request. The College 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 College gets the request, it must notify the individual in writing that the College has complied or intends to comply with their objections or that the College 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 College and the individual;

- required or authorised by Data Protection Laws; or

- based on the individual's explicit consent.

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

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

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

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

18 Marketing And Consent

The College will sometimes contact individuals to send them marketing or to promote the College. Where the College 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.

Shipley College 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 College 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 College 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 College is marketing its own similar services; and
- the College 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. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that it can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale e.g. CCTV cameras.

All DPIAs must be reviewed and approved by the College Data Protection Officer.

20 Transferring Personal Data To A Country Outside The EEA[1]

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 College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

[1] EEA still applies to the UK during the transition period as part of the Brexit withdrawal agreement, and confirmation of its impact will be confirmed prior to its end on 31/12/20.

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

21 Monitoring and Reporting

The Policy will be monitored by the DPO and reported to SMT on a regular basis.

22 Links to other Policies & Procedures

This Policy links to all College Policies and Procedures where personal and sensitive personal data is integral to them.

Whistleblowing Policy and Procedure
Payment Card Information Security Policy - copy available from the finance office
Financial Regulations and Annexes
Salt Foundation Data Protection Policy

Appendix 1 - Data Retention Schedule

Appendix 2 - Definitions

College– Shipley College, Salt Building, Victoria Road, Saltaire, BD18 3LQ

College Employees – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary employees hired to work on behalf of the College.

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 College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College 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.

Data Protection Officer – Shipley College Data Protection Officer is Ian Durham, and can be contacted at: DPO@shipley.ac.uktelephone 7253.

Data Protection Leads - These are the Vice Principal Finance and Planning, the Director of Physical Resources and the HR Manager who will act on behalf of the Data Protection Officer if required.

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 College 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

Where there is a data breach within the College, it is a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to College. This Procedure should be read in conjunction with our Data Protection Policy (Page 7)

This Procedure must be followed by all staff. At all stages of this Procedure, the College Data Protection Officer and Senior Management Team will decide whether to seek legal advice. This Procedure will also apply where the College is notified by any third parties that process Personal Data on its behalf that they have had a data breach which affects the College's Personal Data.

The Procedure is set out below. Any failure to follow this Procedure may result in disciplinary action.

1 IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, however big or small, you must report this to the College Data Protection Officer immediately. The College Data Protection Officer is Ian Durham, and can be contacted at: DPO@shipley.ac.uk telephone 7253. Any other questions about the operation of this Procedure or any concerns that the Procedure has not been followed should be referred in the first instance to the College Data Protection Officer.

You can report a breach using the Data Protection Breach Form which can be accessed by the College staff portal. Completion of this form will notify the College Data Protection Officer and the Data protection leads who will respond to the breach if the Data Protection Officer is unavailable. These are the Vice Principal Finance and Planning, the Director of Physical Resources and the HR Manager.

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches must be reported. False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable the College to learn lessons in how we respond and the remedial action to put in place.

The College has a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach.

2 BECOMING AWARE OF A DATA BREACH – INVESTIGATING

The College becomes aware of a data breach when it has a reasonable degree of certainty that a security incident has occurred that has led to Personal Data being compromised. From this point, the time limit for notification to the ICO will commence.

When you report a data breach to the College Data Protection Officer, the College Data Protection Officer will promptly investigate the breach to ascertain whether the College is fully aware that a breach has occurred that has led to Personal Data being compromised.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

3 ASSESSING A DATA BREACH

Once you have reported a breach and the College Data Protection Officer has investigated it and has decided that the College is aware that a breach has occurred, the College Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, the College Data Protection Officer will notify management. If necessary, the College will appoint a response team which may involve, for example, our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

The College will then investigate the breach and consider any on-going risks to the College and any individuals affected.

If the College Data Protection Officer and management consider that the breach is very serious, they will consider the impact on the College reputation and the effect it may have on the trust placed in us. The College Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.

4 FORMULATING A RECOVERY PLAN

The College Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, the College Data Protection Officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.

5 NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, the College must notify the breach to the ICO within 72 hours of becoming aware of the breach. We must also notify the individuals concerned, as soon as possible, where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by the College Data Protection Officer in line with the College Data Breach Policy, and the notification will be made by the College Data Protection Officer – please be aware that under no circumstances must you try and deal with a data breach yourself.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

6 NOTIFYING A DATA BREACH TO INDIVIDUALS

The College must also notify the individuals concerned, as soon as possible, where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by the College Data Protection Officer in line with the College Data Breach Policy and in conjunction with consulting the ICO, if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that under no circumstances must you try and deal with a data breach yourself.

In some circumstances, explained in the College Data Breach Policy, we may not need to notify the affected individuals. The College Data Protection Officer will decide whether this is the case.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.

7 NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

The College may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach.

The decision as to whether any third parties need to be notified will be made by the College Data Protection Officer and management. They will decide on the content of such notifications.

THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.

8 CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

The College needs to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our College Data Protection Officer will consider whether we need to update the ICO about the data breach.

THIS WILL BE CONSIDERED ON AN ONGOING BASIS.

9 EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the College learns from previous incidents.

It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. The College Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.