Quality System

Policy Number

POL-DP-01

Policy Title

General Data Protection Regulation Policy

Written by:	Checked by:	Equality Impact Assessed by:
		
Author: *Vicky Nelson*	Manager: Lee Phillips	Assessor: *Vicky Nelson*

European Union
European Social Fund

General Data Protection Regulation Policy

1.0 Introduction

Bishop Auckland College/South West Durham Training's (thereafter to be termed 'the Organisation') reputation and future growth are dependent on the way the Organisation manages and protects personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the Organisation.

As an Organisation that collects, uses and stores personal data about its employees, students, governors, parents and visitors, the Organisation recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with the Organisation obligations under Data Protection Laws and in particular article 5 of the UK General Data Protection Regulation (UK GDPR).

The Organisation has implemented this policy to ensure all organisation personnel are aware of what they must do to ensure the correct and lawful treatment of personal data. This will maintain confidence in the Organisation and will provide for a successful working and learning environment for all.

Organisation personnel will receive a copy of this policy when they start and may receive periodic revisions of the policy. This policy does not form part of any member of the Organisation's personnel contract of employment and the Organisation reserves the right to change this policy at any time, but it is a condition of employment that organisational personnel will abide by the rules and polices made by the Organisation. Any failures to follow the policy may result in disciplinary action.

If you have any queries concerning this policy, please contact the Data Protection Officer (DPO).

2.0 About this Policy

This policy (and the other policies and documents referred to in it) sets out the basis on which the Organisation will collect and use personal data either where the Organisation collects it from individuals itself or where it is provided to the Organisation by third parties. It also sets out rules on how the Organisation uses, transfers and stores personal data. This Policy applies to all personal data stored electronically, in paper form or otherwise.

3.0 Definitions

3.1 Organisation – is made up of Bishop Auckland College, Bishop Auckland College Nursery and South West Durham Training.

3.2 Organisation Personnel – any employee, worker or contractor of the Organisation who accesses any of the Organisation's personal data and will include employees, consultants, contractors and temporary personnel hired to work on behalf of the Organisation.

3.3 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 Organisation is the Controller of include employee details or information the organisation collects relating to students. The Organisation will be viewed as a Controller of personal data if it decides what personal data the Organisation 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.

3.4 Data Protection Laws – The UK 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.

3.5 Data Protection Officer (DPO) – our DPO is Vicky Nelson, and can be contacted on extension 3282 or DPO@bacoll.ac.uk

3.6 Data Asset Owner (DAO) - A member of the Organisation's personnel who has senior responsibility for ensuring that specific data assets are handled and managed appropriately. This includes personal data and non-personal information that is critical to the organisation. Data assets can be held in paper as well as electronic formats.

3.7 Information Commissioner's Office (ICO) – the ICO is the UK's data protection regulator.

3.8 Individuals/data subject – living individuals who can be identified, *directly* or *indirectly*, from information that the Organisation 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.

3.9 Personal Data – any information about an individual (see 3.8) which identifies them or allows them to be identified in conjunction with other information that is held.

Personal data is defined broadly and covers things such as name, address, email address (including a business context, email address 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 in 3.11. Special categories of personal data are given extra protection by Data Protection Laws.

3.10 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 the 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.

3.11 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.

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

4.0 Registration as a Data Controller

The organisation is required to register with the Information Commissioner's Office ICO as a Data Controller and to pay a registration fee each year. Details of the organisation's registrations are published on the Information Commissioner's website:
https://ico.org.uk/ESDWebPages/Entry/Z7686647 for BAC
https://ico.org.uk/ESDWebPages/Entry/Z5426193 for SWDT

5.0 The Organisations obligations

5.1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural person's, the Organisation shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the UK GDPR.

5.2 The Organisation must ensure that it integrates data protection into its policies and procedures

5.3 The organisation must ensure the designation of a suitable DPO, on the basis of professional qualities, and in particular, expert knowledge of data protection law and practices and the ability to fulfil the responsibilities referred to in 6.2.

5.4 The organisation must ensure that the DPO has direct access to the Board/Principal Chief Executive, circumnavigating normal lines of command.

5.5 The Organisation must ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

5.6 The Organisation shall support the DPO in performing the tasks referred to in 6.2, providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain their expert knowledge.

5.7 The Organisation shall ensure that the DPO has full independence to perform their tasks.

5.8 The organisation must ensure that any other tasks and duties assigned to the DPO do not result in a conflict of interest.

5.9 The organisation will ensure that data protection is reviewed and monitored through Corporate Board, Directorate and Senior Leadership Management Team (SLMT) meetings. An annual summary report on Data Protection will be presented at Corporate Board and SLMT.

6.0 Responsibilities

6.1 Principal/ Chief Executive responsibilities

6.1.1 The Principal/ Chief Executive has overall responsibility for ensuring our organisation is compliant with this Policy and with Data Protection Legislation**.**

6.2 Data Protection Officer DPO responsibilities

6.2.1 The DPO is responsible for:

(a) day-to-day responsibility for monitoring compliance with this Policy and GDPR legislation
(b) advising the organisation on data protection matters
(c) informing and advising organisation personnel, who carry out processing, of their obligations pursuant to the GDPR.
(d) providing guidance where required on the completion of data protection impact assessments
(e) cooperating with and acting as the contact point for the ICO
(f) receiving reports of data incidents for escalation as appropriate.

(g) Maintaining records of processing activities
(h) Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.
(i) Maintaining a GDPR Risk Register to identify and assess the threats and high level risks to the processing of personal data within the organisation. Reviewing technical and organisational measures and processes that are in place and assigning additional actions as required to reduce the impact and probability of the risk and protect the confidentiality, integrity and availability of personal data.

6.3 Data Asset Owner responsibilities

6.3.1 DAO's are responsible for ensuring that they carry out their duties as set out in the Data Asset Owner handbook (ref DP-DA-01) including:

(a) Ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and data protection legislation.
(b) Having an overview of any processing activities that occur within their work area, including the repositories that hold personal data and ensure these are documented on a comprehensive Departmental Data Asset Register
(c) Ensuring that data assets are processed in line with the Data Protection Principles
(d) Knowing who has access to their data assets and why, and ensuring the use of the asset is monitored.
(e) Acting as an advocate for issues relating to data protection and privacy, including raising awareness, promoting good practice and challenging poor practice within their work area. Ensuring that their staff are aware of their data protection responsibilities, including ensuring they undertake GDPR/ Data Protection training as required.
(f) Reviewing the data assets, they are responsible for and assessing them against risk, to ensure the Confidentiality, Integrity and Availability of these assets, including those in their delivery chain, are maintained at all times
(g) Undertaking compliancy checks/ audits as required to ensure the confidentiality, integrity and availability of their data assets/ Organisational assets are maintained at all times
(h) Ensuring Data Protection by Design principles are applied to new systems and business processes, including undertaking Data Protection Impact Assessments (DPIAs) as appropriate for data processing activities, within their business area
(i) Understanding where and when data is shared with third parties and ensuring suitable GDPR contracts and data sharing agreements are in place as required.
(j) Recognising actual or potential security incidents and **Data Breaches** and consulting with the Data Protection Officer (DPO) on incident management.
(k) Assisting the DPO in their duties through providing all appropriate information and support as required by the DPO and consulting with the DPO in a timely manner on new developments or issues affecting the use of personal data in the organisation

6.4 Organisation Personnel responsibilities

6.4.1 All Organisation personnel must comply with this policy and are responsible for understanding and complying with relevant policies and processes regarding the handling of personal data appropriate to their role.

6.4.2 Organisation personnel must ensure that they keep confidential any personal data that they collect, store, use and come into contact with during the performance of their duties.

6.4.3 Organisation personnel must not release or disclose any personal data:

(a) Outside the Organisation, to any unauthorised third party – Please see Section 13- Data Sharing and refer to 'Key questions for information sharing' (ref DP-IS-01).

(b) Inside the Organisation, to Organisation 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.

6.4.4 Organisation personnel must take all steps to ensure there is no unauthorised access to personal data whether by other Organisation personnel who are not authorised to see such personal data or by people outside the Organisation.

6.4.5 Organisation personnel must ensure that they do not access any personal information through the organisation's Management Information Systems (MIS) unless they are authorised to do so and it is a requirement as part of their role.

6.4.6 Organisation personnel must ensure they abide by the Organisations Clean Desk Policy (ref POL-DP-20) to ensure that any personal data they come in contact with is processed securely and confidentially.

6.4.7 Organisation personnel must also refer to the following organisational Data Protection guidance documents in relation to the processing of personal data:

(a) Departmental Data Asset Registers (ref DP-DAR-01)
(b) Relevant Data Sharing Agreements (ref DP-DSA-01)
(c) The GDPR Dos and Don'ts (ref DP-DD-01)
(d) Staff guidelines on the transit/transfer/sharing of restricted and confidential information (ref DP-IS-02)
(e) Key Questions for Information Sharing (ref DP-IS-01)
(f) Retention Policy (POL-DP-04
(g) Remote Working Policy (POL-IT-08)

6.4.8 Organisation personnel are responsible for immediately reporting any data incidents, no matter how big or small to the DPO, by completing a data breach notification form (ref DP-DB-02) or by clicking on the Data Breach notification icon on the staff portal and completing the online notification form.

6.4.9 Organisation personnel must ensure that personal data is kept in accordance with the organisations retention policy (ref POL-DP-04) and departmental Data Asset Registers.

6.4.10 Organisation personnel must ensure that they undertake any data protection training as required by the organisation

7.0 Data Protection Principles

7.1 When using personal data, Data Protection Laws require that the Organisation complies with the following principles. These principles require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (refer to section 8- Lawful use of personal data and section 9 Transparent Processing- Privacy Notices)

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

(c) Adequate, relevant and limited to what is necessary for the purposes for which it is being processed.

(d) 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 (refer to section 10 Data Quality)

(e) Kept for no longer than is necessary for the purposes for which it is being processed (refer to section 11- Retention of personal data)

(f) 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 (refer to section 12- Data Security and Section 13 Data sharing)

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

7.3 In addition to complying with the above requirements, the Organisation also has to demonstrate in writing that it complies with them. The Organisations has a number of policies and procedures in place, including this policy and the documentation referred to in it, to ensure that the Organisation can demonstrate its compliance.

8.0 Lawful use of Personal Data

8.1 In order to collect and/or use personal data lawfully, the Organisation needs to be able to show that its use meets one of a number of legal grounds:

(a) Consent – the individual has given clear consent for the Organisation to process their personal data for a specific purpose.

(b) Contract – the processing is necessary for a contract the Organisation has with the individual or because they have asked the Organisation to take specific steps before entering into a contract.

(c) Legal Obligation – the processing is necessary for the Organisation to comply with the law (not including contractual obligations).

(d) Vital interests – the processing is necessary for the Organisation to protect someone's life.

(e) Public task – the processing is necessary for the Organisation to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests – the processing is necessary for the Organisation's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this cannot apply to public authorities processing data to perform official tasks).

8.2 In addition, when the Organisation collects and/or uses special categories of personal data, the Organisation has to show that one of a number of additional conditions is met:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition many not be lifted by the data subject.

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(e) Processing relates to personal data which are manifestly made public by the data subject

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(h) Processing is necessary for purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and the services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.

(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

(j) Processing is necessary for archiving purposes in the public interest scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8.3 The Organisation has carefully assessed how it uses personal data and how it complies with the lawful basis for processing as set out in 8.1 and 8.2.

9.0 Transparent Processing – Privacy Notices

9.1 Where the Organisation collects personal data directly from individuals, the Organisation will inform them about how the Organisation uses their personal data. This is in a privacy notice, which is issued at the point of collection. The Organisation has adopted the following privacy notices:

- Privacy Notice – Student and Prospective Students (ref: DP-PN-01)
- Privacy Notice – Recruitment (ref: DP-PN-02)
- Privacy Notice – Staff (ref: DP-PN-03)
- Privacy Notice – Bishop Auckland College Child-Care Services – Nursery (ref DP-PN-04)
- Privacy Notice – Hair and Beauty Client (DP-PN-06)
- Privacy Notice – Visitors and Contractors (DP- PN-07)

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

9.3 If the Organisation changes how it uses personal data, the Organisation may need to notify individuals about the change. If Organisational personnel intend to change how they use personal data the DPO must be notified. The DPO will then assess whether there is an appropriate lawful basis for changing the way in which the personal data is used, if amendments to the privacy notice are required and if amendments are required to any other controls which apply.

10.0 Data Quality – Ensuring the use of accurate, up to data and relevant Personal Data

10.1 Data Protection Laws require that the Organisation 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 (section 9.0) and as set out in the Organisation's record of how it uses personal data. The Organisation is also required to ensure that the personal data it holds is accurate and kept up to date.

10.2 All Organisation personnel that collect and record personal data shall ensure that the personal data is recorded accurately, 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.

10.3 All Organisation personnel that obtain personal data from sources outside the Organisation 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 Organisation personnel to independently check the personal data obtained.

10.4 In order to maintain the quality of personal data, all Organisation personnel that 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 the Organisation must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

10.5 The Organisation recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The Organisation has a Data Subject Individual Rights Procedure (ref: BAC-DP-01), which sets out how the Organisation responds to requests relating to individual rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

10.6 Any request received from an individual relating to any of the above rights, in relation to their personal data, should be dealt with in accordance with the Data Subject Individual Rights procedure. All requests must be forwarded to the Quality Office, who will ensure that appropriate actions are taken and a response issued without undue delay and at least within one month.

11.0 Retention of Personal Data

11.1 Data Protection Laws require that the Organisation does not keep personal data longer than is necessary for the purpose or purposes for which the Organisation collected it.

11.2 The Organisation has assessed the types of personal data that it holds and has set retention periods for the different types, along with the method of deletion/disposal. These are set out in the Data Retention Policy (ref: POL-DP-04).

11.3 If Organisation personnel 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 (ref: POL-DP-04), for example because there is a requirement by law, or if the Organisation personnel have any questions about this policy or the Organisation's personal data retention practices, they should contact the DPO for guidance.

11.4 Each department has a Data Asset Register (ref DP-DAR-01). This document clearly defines each process a department is involved in, what personal data is processed along with the required storage, retention and method of disposal of such data. Managers are required to ensure the Organisation personnel they line manage are aware of this document and where to locate it.

12.0 Data Security

12.1 The Organisation takes information security very seriously and the Organisation has security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. The Organisation has in place the Information Security Policy (ref: POL-IT-06) and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Clean Desk Policy (ref POL-DP-02) is also in place to protect the security and confidentiality of all information that is processed by organisation personnel.

13.0 Data Sharing

13.1 Before any personal data can be shared with an external third party, organisational personnel must ensure that they have a clear and legitimate purpose for sharing the information and they must ensure they have appropriate permissions/ approval to do so. This must be in the form of, one of following:

(a) A legal obligation/ statutory requirement to share
(b) GDPR contract and due diligence paperwork in place
(c) A relevant signed data sharing agreement in place
(d) Consent from the data subject, in the form of a signed 'Permission to disclose personal data form' (ref DP-PD-01) or a signed declaration
(e) A signed Police disclosure form with clear reasons to warrant the disclosure/ Court order
(f) Sufficient public interest to share i.e. safeguarding/ Prevent agenda

13.2 Organisation personnel must note that even when information can be shared, the information may only be permitted to be shared by key personnel within the organisation i.e. Safeguarding Officer, Duty Manager, Data Protection Officer/ designate. Please refer to the 'Key Questions for information sharing' (ref DP-IS-01) for further information on the sharing of personal information or if in doubt speak with your line manager or the DPO.

14.0 Data Incident/ Breach

14.1 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 Organisation personnel must comply with the Organisation's Data Breach Policy (ref: POL-DP-03) and Data Breach Notification Process (ref: DP-DB-01).

14.2 A personal data breach is defined very broadly and is effectively any failures 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. Most personal data breaches happen as a result of something someone internal does.

14.3 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 Organisational personnel 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 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 encryption key.

- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

14.4 All data incidents/breaches must be reported to the DPO using the Data Breach Notification form (ref DP-DB-02). It is the responsibility of all organisational personnel to report a data incident no matter how big or small.

14.5 All data incidents/ breaches must be documented on an internal data breach register held by the DPO.

15.0 Training of Organisation Personnel

15.1 All Organisation personnel who process personal data will receive data protection training. Training is important to reduce the likelihood of misuse of personal data. All Organisational personnel at induction will receive training about data protection and will be required to undertake annual refresher training.

15.2 All Data Protection Policies, Procedures and Documents are accessible to organisational personnel within a dedicated central location on the staff portal for ease of access and reference.

15.3 Regular informative emails will be sent out to organisational personnel by the DPO to keep them up to date with current data protection matters and reminders.

16.0 Appointing Contractors who access the Organisation's Personal Data

16.1 If the Organisation appoints a contractor/supplier who is a processor of the Organisation's personal data, Data Protection Laws require the Organisation only appoints them where the Organisation has carried out sufficient due diligence and only where the Organisation has appropriate contracts in place.

16.2 One requirement of the UK GDPR is that a controller must only use processors who meet the requirements of the UK 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.

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

16.4 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 the Organisation, as controller, remains responsible for what happens to the personal data.

16.5 UK GDPR requires the contract with the processor to contain the following obligations as a minimum, to:

- Only act on the written instructions of the controller
- Not export personal data without the controller's instruction
- Ensure staff are subject to confidentiality obligations
- Take appropriate security measures
- Only engage sub-processors with the prior consent (specific or general) of the controller and under a written contract
- Keep the personal data secure and assist the controller to do so
- Assist with the notification of data breaches and data protection impact assessments
- Assist with subject access/individual rights requests
- Delete/return all personal data as requested at the end of the contract
- Submit to audits and provide information about the processing
- To tell the controller if any instruction is in breach of the UK GDPR or other EU or member state data protection law

16.6 In addition the contract should set out the:

- Subject matter and duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of individuals
- Obligations and rights of the controller

17.0 Individuals' Rights

17.1 The UK GDPR gives individuals more control about how their data is collected and stored and what is done with it. See clause 10.5 for more detail. The Data Subject Individual Rights Procedure (ref: BAC-DP-01) details the process for data subjects exercising their rights.

17.2 The Organisation will ensure that individuals (data subjects) can exercise their rights in accordance with procedure BAC-DP-01.

18.0 Marketing and Consent

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

18.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals.

18.3 Where an individual is contacted for marketing purposes, consent must be obtained. Consent is central to electronic marketing. Best practice is to provide an un-ticked opt-in box.

19.0 Automated Decision Making and Profiling

19.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to individuals:

- Automated Decision Making – happens where the Organisation 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 the Organisation automatically uses personal data to evaluate certain things about an individual.

19.2 Any automated decision making or profiling which the Organisation carries out can only be done once the Organisation is confident that it is complying with Data Protection Laws. If Organisation personnel, therefore, wish to carry out any automated decision making or profiling they must inform and gain approval of the DPO.

19.3 The Organisation does not carry out automated decision making or profiling in relation to Organisational personnel or students.

20.0 Data Protection Impact Assessment (DPIA)

20.1 The UK GDPR requires organisations 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 (ref DP-IA-01). 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/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
- Implement measures to address the risks

20.2 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.

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

20.4 Where the Organisation is launching or proposing to adopt a new process, product or service which involves personal data, the Organisation needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The Organisation needs to carry out a DPIA at an early stage in the process, so 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.

20.5 Situations where the Organisation may have to carry out a DPIA include the following (this list is not exhaustive):

- Large scale and systematic use of personal data for the purposes of automated decision making or profiling 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
- Systematic monitoring of public areas on a large scale e.g. CCTV camera

20.6 All DPIA's must be reviewed and approved by the DPO.

21.0 Transferring Personal Data to a Country outside the EEA

21.1 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 Organisation appoints a supplier outside the EEA which may give access to the personal data to staff outside the EEA.

21.2 So that the Organisation can ensure it is compliant with Data Protection Laws, Organisation personnel must not export personal data unless it has been approved by the DPO.

21.3 Organisation personnel must not export any personal data outside the EEA without the approval of the DPO.

22.0 Conclusion

22.1 Compliance with the UK GDPR and the Data Protection Act 2018 is the responsibility of all Organisation personnel. Any deliberate breach of this GDPR Policy may lead to disciplinary action being taken or even criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be referred to the Data Protection Officer.

For further information, contact

Vicky Nelson
Data Protection Officer / Quality Assurance Manager

September 2022