Quality Management System

Policy Number

POL-DP-01

Policy Title

Data Protection Policy

Document Author	Vicky Nelson Quality Assurance Manager/Data Protection Officer
Approved By	Lee Phillips Director of Quality and HE
Version	Issue 2 Rev 1
Effective from	September 2026
Last reviewed	September 2026
Next review due	September 2027
Equality Impact Assessed	September 2026

Alternative Format Statement

We are committed to ensuring all our materials are accessible to everyone. If you require this document in an alternative format please contact:

Quality Improvement Team
Email: Quality@bacoll.ac.uk
Phone: 01388 443069

Please note: On our website we have the Recite Accessibility toolbar. If you select Accessibility on the top toolbar, any text on the website, including linked policies and procedures can:

- be converted from text to speech
- be translated into over 100 languages including 65 text to speak voices
- have its colour, scheme, text, font style, size and spacing changed

Contents

Section and Title	Page Number
Alternative Format Statement	2
1.0 Introduction/Scope	5
2.0 About this Policy	5
3.0 Definitions	6
4.0 Registration as a Data Controller	8
5.0 Bishop Auckland College Group's obligations	8
6.0 Responsibilities	8
6.1 Principal/ Chief Executive responsibilities	8
6.2 Data Protection Officer DPO responsibilities	9
6.3 Data Asset Owner responsibilities	9
6.4 All users of personal data responsibilities	10
7.0 Data Protection Principles	12
8.0 Lawful use of Personal Data	13
9.0 Transparent Processing – Privacy Notices	14
10.0 Data Quality –accurate, up to data and relevant	14
11.0 Retention of Personal Data	15
12.0 Data Security	16
13.0 Data Sharing	16
14.0 Data Incident/ Breach	17
15.0 Training for all users of personal data	18
16.0 Appointing Contractors who access BACG's Personal Data	19
17.0 Individuals' Rights	19
18.0 Marketing and Consent	19
19.0 Automated Decision Making and Profiling	20

20.0 Data Protection Impact Assessment (DPIA) 20

21.0 Transferring Personal Data to a Country outside the EEA 21

22.0 Conclusion 21

Contact Information 22

Summary of significant changes 22

Data Protection Policy

1.0 Introduction/Scope

Bishop Auckland College Group (thereafter to be termed 'BACG'), collects, uses and stores personal data about various categories of individuals. BACG 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 article 5 of the UK General Data Protection Regulation (UK GDPR).

This policy applies to all personal data, including special categories of personal data, processed by BACG, including data on employees, students, applicants, governors, parents, visitors, volunteers and other stakeholders.

This policy applies to 'all users' (ref 3.2) working for or on behalf of BACG who obtains, users, accesses or stores personal data, regardless of their role, grade or type of contract. All users – includes but is not limited to, employees, consultants, contractors, volunteers and temporary personnel hired to work on behalf of BACG. It also applies to students who process personal data on behalf of BACG or as a requirement of their studies. Adherence to this policy is mandatory for all users. Any failure to follow the policy may result in disciplinary action.

BACG has implemented this policy to ensure all users of personal data are aware of what they must do to ensure the correct and lawful treatment of personal data. Ensuring the delivery of BACGs commitment in protecting the rights and privacy of individuals by safeguarding their personal data.

2.0 About this Policy

This policy (and the other policies and documents referred to in it) sets out the basis on which BACG will collect and use personal data, either where BACG collects it from individuals itself or where it is provided by third parties. It also sets out rules on how the BACG 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 BACG – Bishop Auckland College Group, is made up of Bishop Auckland College, Durham Gateway, McIntyre Centreand South West Durham Training.

3.2 All users – includes but is not limited to, employees, consultants, contractors, volunteers and temporary personnel hired to work on behalf of Bishop Auckland College Group who obtains, uses, accesses or stores personal data, regardless of their role, grade or type of contract. It also applies to students who process personal data on behalf of BACG or as a requirement of their studies.

3.3 Controller – any entity (e.g. company, organisation, public authority or person), which alone or jointly with others, determines the purpose and means of processing of personal data and makes its own decisions about how it is going to collect and use personal data.

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 BACG'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 BACG. 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, but not limited to, 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

3.10 Processor – any entity (e.g. company, organisation or person) which accesses or uses personal data on the instruction of a Controller.

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

BACG 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 Bishop Auckland College Group's 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, BACG 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 BACG will ensure that it integrates data protection into its policies and procedures

5.3 BACG will ensure the designation of a suitable Data Protection Officer (DPO), in accordance with Section 4 Article 37 of the UK GDPR and will ensure the DPO is supported and has the resources in accordance with Article 38, to be able to fulfil their responsibilities, as referred to in 6.2 below and in accordance with Section 4 Article 39 of the UK GDPR.

5.4 BACG 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 BACG 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:

- advising and monitoring BACG on all matters with respect to data protection compliance in regards to this Policy and data protection law.
- informing and advising all users, who carry out processing of personal data, of their obligations pursuant to the UK GDPR.
- providing guidance where required on the completion of data protection impact assessments
- cooperating with and acting as the contact point for the ICO
- receiving reports of data incidents for escalation as appropriate.
- Maintaining records of processing activities
- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.
- Maintaining a GDPR Risk Register to identify and assess the threats and high level risks to the processing of personal data within BACG. 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 to 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-DAO-01) including:

- Ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and data protection legislation.
- 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
- Ensuring that data assets are processed in line with the Data Protection Principles
- Knowing who has access to their data assets and why, and ensuring the use of the asset is monitored.

- 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.
- 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
- Undertaking compliancy checks/ audits as required to ensure the confidentiality, integrity and availability of their data assets/ BACGs assets are maintained at all times
- 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
- Understanding where and when data is shared with third parties and ensuring suitable GDPR contracts and data sharing agreements are in place as required.
- Recognising actual or potential security incidents and Data Breaches and consulting with the Data Protection Officer (DPO) on incident management.
- 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 BACG.

6.4 All users of personal data responsibilities

6.4.1 All users of personal data must:

- Comply with this policy and are responsible for understanding and complying with other relevant policies and processes regarding the handling of personal data appropriate to their role.
- They 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.

- They must take all steps to not disclose or allow unauthorised access to any personal data:
  (a) Outside BACG, to any unauthorised third party – Please see Section 13.0- Data Sharing and refer to 'Key questions for information sharing' (ref DP-IS-01).
  (b) Inside BACG, to anyone 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.
- Must ensure that they do not access any personal information through BACG's Management Information Systems (MIS) unless they are authorised to do so and it is a requirement as part of their role.
- Ensure they abide by BACG's Clean Desk Policy (ref POL-DP-20) to ensure that any personal data they come in contact with is processed securely and confidentially.
- Refer to the following BACG Data Protection guidance documents in relation to the processing of personal data:
  - Departmental Data Asset Registers (ref DP-DAR-01)
  - Relevant Data Sharing Agreements (ref DP-DSA-01)
  - The GDPR Dos and Don'ts (ref DP-DD-01)
  - Staff guidelines on the transit/transfer/sharing of restricted and confidential information (ref DP-IS-02)
  - Key Questions for Information Sharing (ref DP-IS-01)
  - Data Retention Policy (POL-DP-04
  - Remote Working Policy (POL-IT-08)
- Immediately report 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.
- ensure that personal data is kept in accordance with BACG's retention policy (ref POL-DP-04) and departmental Data Asset Registers.
- ensure that they undertake any data protection training as required by BACG.

7.0 Data Protection Principles

7.1 BACG will ensure adherence to the data protection principles in all processing of personal data. These principles require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (refer to section 8- Lawful use of personal data and section 9 Transparent Processing- Privacy Notices)
- 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 (refer to section 10 Data Quality)
- Kept for no longer than is necessary for the purposes for which it is being processed (refer to section 11- Retention of personal data)
- 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, BACG also has to demonstrate in writing that it complies with them. BACG has a number of policies and procedures in place, including this policy and the documentation referred to in it, to ensure that it can demonstrate its compliance.

8.0 Lawful use of Personal Data

8.1 BACG is committed to ensuring that all personal data is processed lawfully, fairly, and transparently, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

BACG will only collect and process personal data where there is a valid legal basis. These include:

- The data subject has given clear consent for the processing of their personal data for a specific purpose;
- The processing is necessary for the performance of a contract with the data subject;
- The processing is necessary to comply with a legal obligation;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or
- The processing is necessary for the purposes of legitimate interests pursued by BACG or a third party, except where overridden by the interests or fundamental rights and freedoms of the data subject. (This cannot apply to public authorities processing data to perform official tasks).

Where consent is relied upon, it will be obtained in a clear and specific manner, and individuals will have the right to withdraw consent at any time.

8.2 In addition, when BACG collects and/or uses special categories of personal data (ref 3.11), it will ensure an additional condition is met at set out in the Article 9(2) of the UK GDPR.

8.3 BACG 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 BACG collects personal data directly from individuals, it will inform them about how BACG uses their personal data. This is in a privacy notice, which is issued at the point of collection. BACG 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- Individual Advise and Guidance (IAG) Customers (DP-PN-05)
- Privacy Notice – Hair and Beauty Client (DP-PN-06)
- Privacy Notice – Visitors and Contractors (DP- PN-07)
- Privacy Notice – Prospective Governors and Governors (DP-PN-08)
- Privacy Notice – Parent-Carer (DP-PN-09)
- Privacy Notice – Employer (DP-PN-10)
- Privacy Notice – McIntyre Restaurant Customers (DP-PN-11)

The above privacy notices can be found on the Data Protection page on the BAC website.

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

9.3 If BACG changes how it uses personal data, it may need to notify individuals about the change. If BACG 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 –accurate, up to data and relevant

10.1 BACG 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).

10.2 All users of personal data 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. Please note that this does not apply to personal data which BACG must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

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

10.3.1 The right to be informed
10.3.2 The right of access
10.3.3 The right to rectification
10.3.4 The right to erasure
10.3.5 The right to restrict processing
10.3.6 The right to data portability
10.3.7 The right to object
10.3.8 Rights in relation to automated decision making and profiling

10.4 Any request received from an individual relating to any of the above rights, in relation to their personal data, will 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 BACG does not keep personal data longer than is necessary for the purpose or purposes for which it was collected.

11.2 BACG 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 users of personal data 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, 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 that the staff they line manage are aware of this document and where to locate it.

12.0 Data Security

12.1 BACG takes information security very seriously and has implemented appropriate security measures to prevent unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. BACG has in place an 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 all users.

13.0 Data Sharing

13.1 Before any personal data can be shared with an external third party, all users of personal data 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 legal obligation/ statutory requirement to share
- GDPR contract and due diligence paperwork in place
- A relevant signed data sharing agreement in place

- 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
- A signed Police disclosure form with clear reasons to warrant the disclosure/ Court order
- Sufficient public interest to share i.e. safeguarding/ Prevent agenda

13.2 All users of personal data must note that even when information can be shared, the information may only be permitted to be shared by key personnel within BACG 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 BACG 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 all users of personal data must comply with BACGs 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.

There are three main types of personal data breach which are as follows:

14.2.1 Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that users of personnel data are 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.

14.2.2 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.

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

14.3 All data incidents/breaches must be reported to the DPO immediately on discovering a data breach or suspecting a potential data incident has occurred, using the Data Breach Notification form (ref DP-DB-02). It is the responsibility of all users of personal data to report a data incident no matter how big or small.

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

14.4 The DPO with assistance from relevant staff/directorate as required will undertake an investigation and complete a report. Where the data breach is reportable 'the breach results in a risk to the rights and freedoms of the data subject' the DPO will notify the Information Commissioner's Office (ICO), within 72 hours after becoming aware of the data breach.

15.0 Training for all users of personal data

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

15.2 All Data Asset Owners (DAOs), members of BACG's personnel who have senior responsibility for data assets, will receive DAO training from the DPO. This training will be centred around the Data Asset Owner Handbook (ref DP-DAO-01), to ensure they understand their roles and responsibilities.

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

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

16.0 Appointing Contractors who access BACG's Personal Data

16.1 If BACG appoints a contractor/supplier who is a processor of its personal data, they will only be appointed where sufficient due diligence has been carried out and only where appropriate contracts are in place.

16.2 Where BACG appoints a processor the contract will be in writing. These contracts set out the mandatory terms and obligations of the data processor, as detailed in Article 28(3) of the UK GDPR.

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 10.3 for more detail. The Data Subject Individual Rights Procedure (ref: BAC-DP-01) details the process for data subjects exercising their rights.

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

18.0 Marketing and Consent

18.1 BACG will sometimes contact individuals to send them marketing or to promote the organisation. Where BACG carries out any marketing it will make sure 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 a decision is made 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 Before any automated decision making or profiling can be carried out by BACG, approval must be gained from the DPO, to ensure compliancy with Data Protection Laws.

19.3 BACG does not currently carry out automated decision making or profiling in relation to any of its stakeholders.

20.0 Data Protection Impact Assessment (DPIA)

20.1 BACG is committed to protecting the rights and freedoms of individuals when processing personal data. Where processing is likely to result in a high risk to individuals' privacy—such as the use of new technologies, large-scale processing of special category data, or systematic monitoring—a Data Protection Impact Assessment (DPIA) (ref DP-IA-01), will be undertaken in accordance with Article 35 of the UK GDPR.

20.2 The DPIA process helps the College:

- Assess the necessity and proportionality of processing
- Identify and mitigate risks to data subjects

- Demonstrate compliance with data protection principles

20.3 All staff must consult the Data Protection Officer (DPO) before initiating any project that may require a DPIA.

21.0 Transferring Personal Data to a Country outside the EEA

21.1 BACG will ensure that any personal data transferred outside the UK/EEA is adequately protected in accordance with data protection law. Generally, BACG does not transfer any personal data to countries outside the UK and the European Economic Area (EEA), however if it was necessary for academic, administrative, or operational purposes—for example, when engaging with international students, partner institutions, or third-party service providers. Such transfers will only take place where:

- The UK government (or the European Commission, where applicable) has issued an **adequacy decision** for the country in question; or
- BACG has implemented **appropriate safeguards**, such as **Standard Contractual Clauses (SCCs)**; or
- A specific **derogation** applies under UK GDPR (e.g. the individual has explicitly consented).

Note: 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 BACG appoints a supplier outside the EEA which may give access to the personal data to staff outside the EEA.

21.2 All users of personnel data 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 users of personal data. Any deliberate breach of this Data Protection 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.

Contact Information

For questions or feedback regarding this policy, please contact:

Vicky Nelson
Data Protection Officer
Email: Quality@bacoll.ac.uk
Phone: 01388 443069

Summary of significant changes

For information about changes made to this Policy see the Change log found on our website.