Data Protection Policy

Document Version Control	
Document Title	Data Protection Policy
Version	1.0
Reviewing Committee	Senior Management Team
Approving Committee	Senior Management Team
Policy Lead	Data Protection Officer
Date of Last Review	N/A
Date of Approval	January 2026
Date Effective from	February 2026
Date of Next Review	August 2027

Table of Contents

1. Introduction

VCAD adheres to the UK General Data Protection Regulation and the Data Protection Act 2018. The Information Commissioner's Office (ICO) is the UK regulator for data protection.

To maintain this standard, the College guarantees that data is handled lawfully and ethically, respects individual rights, safeguards personal information, and embeds privacy into its operational systems and procedures.

This document describes the approach VCAD takes in managing personal data belonging to students, employees, Governors and Directors, vendors, users of its website, and other external parties, ensuring full alignment with applicable data protection laws.

2. Legal Framework

The Data Protection Act 2018 ('DPA 2018') provides the legal structure for data protection within the UK.

The UK General Data Protection Regulation ('UK GDPR') became effective on 1 January 2021 and sets out the essential principles, rights, and responsibilities governing most personal data processing activities in the UK.

The Information Commissioner's Office (ICO) serves as the UK's autonomous authority responsible for upholding information rights, offering support and recommendations, encouraging best practices, investigating complaints, and enforcing regulations when necessary. The ICO can be reached at https://ico.org.uk/make-acomplaint/. VCAD's registration number is **ZB496235**.

Appendix A contains definitions of important terms related to data protection, while Appendices B and C detail the legal grounds for processing personal data and sensitive personal data, respectively.

3. Purpose and Scope

The College collects and uses personal data for a range of functions, such as student admissions, academic operations, mandatory reporting, and human resources management. This includes a specific category of personal data referred to as special category data, which encompasses sensitive details like ethnic background, medical information, and sexual identity.

This document explains how the College manages personal data concerning employees, students, and external parties, and it applies to all personnel, contractors, and students who interact with such data. Adherence to this policy is compulsory, and violation10. The result in disciplinary action related to Automated Decision-Making and Profiling 12handling personal data in accordance with the fundamental principles set out in Article 5(1) of the UK General Data Protection Regulation (UK GDPR), which underpin the Data Protection Act 2018 and define the legal standards for data processing. In accordance with these principles[1], VCAD will ensure that personal data is:

4.1 Lawful, Fair and Transparent

Managed in a lawful, fair, and open way with respect to individuals (the data subjects).

The College's Privacy Notice clearly explains how it gathers, uses, and shares data from prospective, current, and former students, and the reasons for doing so. This Notice also helps students understand their rights regarding the personal data held by the College, enabling them to make informed choices about providing such data.

Employees contractually agree to VCAD processing their personal data as needed to fulfil their employment contracts and support the College's operations, which may involve partners, technology providers, government agencies, and other public entities.

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

All VCAD personnel who handle personal data related to students, staff, applicants, alumni, or any other individuals must follow the rules set out in this policy.

4.2 Purpose Limitation

Gathered solely for clear, specific, and lawful reasons.

Data is collected for defined, legitimate purposes and is not used in ways that conflict with those original intentions; additional processing for archival, research, or statistical reasons is not considered incompatible. VCAD only uses personal data for the purposes communicated to the individual at the time of collection. If the College intends to use the data for a new and unrelated reason, the individual will be notified beforehand, and in some cases, their consent may be required.

4.3 Data Minimisation

Sufficient, appropriate, and restricted to what is necessary for the intended use.

VCAD aims to collect or use only the personal data that is strictly necessary for the intended purpose and considers using anonymised or pseudonymised data where possible. Data that is irrelevant or unnecessary will not be collected or processed. Gathering personal data “just in case” it might be useful later is not permitted under current regulations.

4.4 Accuracy

Correct and, when needed, kept current; all reasonable efforts must be made to delete or correct inaccurate personal data promptly, considering the purpose for which it is processed.

Personal data is checked for accuracy when first collected and reviewed regularly thereafter. Mistakes are corrected or removed as needed, although data used in decisions affecting an individual will not be deleted; instead, it will be updated for future use and accompanied by a note explaining the correction.

Before any data is shared, its quality is verified – VCAD will not transmit data that is incorrect, incomplete, or outdated.

4.5 Storage Limitation

Retained in a format that allows identification of individuals only as long as necessary for the intended purpose; data may be kept longer if used solely for archival, research, or statistical reasons, provided that suitable technical and organisational safeguards are in place to protect individual rights and freedoms as required by the GDPR.

Personal data is retained only as long as needed and is managed securely to prevent unauthorised access or loss.

VCAD will securely delete or remove data from its systems once there is no longer a legal, operational, or business need to retain it, consistent with the original reason for its collection.

4.6 Integrity and Confidentiality

Handled in a way that guarantees suitable protection of personal data, including safeguards against unauthorised or illegal processing, as well as accidental loss, damage, or destruction, through the use of appropriate technical and organisational controls.

VCAD secures personal data from unauthorised access, loss, or destruction through a variety of protective measures. All institutional systems and services except for CCTV operate entirely on cloud infrastructure, and the College relies solely on a third-party cloud storage provider under contractual agreements that include secure hosting within the UK or in regions that meet UK data protection standards. For more details on CCTV procedures and storage, refer to the institutional CCTV Policy.

All systems undergo routine vulnerability assessments, and any IT systems developed and implemented by external providers must have current security updates before they are activated.

The College's Information Security Awareness Policy promotes compliance by ensuring staff are properly informed about safeguarding personal data. Staff are responsible for keeping any personal data they manage secure and must not disclose such information—whether verbally, in writing, or inadvertently—to anyone not authorised to receive it. Any physical records containing personal data must be stored in locked cabinets or drawers within rooms that are secured and accessible only to authorised personnel. Personal data must not be transferred by members of staff outside the UK, including through the use of websites or applications hosted on servers outside the UK, unless appropriate authorisation and safeguards are in place.

4.7 Accountability

The data controller is obligated to ensure and demonstrate adherence to the first principle.

The College will retain suitable documentation to verify its compliance with these principles.

4.8 Data Protection by Design and Default

VCAD upholds the principle of data protection by design and default, ensuring that personal data is managed with maximum privacy safeguards.

Data protection by default is tied to the core principles of data minimisation and purpose limitation, requiring that personal data be handled with the highest level of privacy and not exposed to an unlimited number of individuals.

Data protection by design involves proactively incorporating privacy measures into any initiative—such as collecting new data types or launching new systems or procedures for storing or accessing personal data—from the beginning. This ensures that security is a primary consideration rather than an afterthought. It is closely associated with the obligations of record-keeping and accountability.

All staff are expected to use only the minimum amount of personal data necessary for their tasks and to consider using anonymised or pseudonymised data when appropriate.

5. Data Subject Rights

Data Subjects, such as students, staff, and third parties, are entitled to exercise their rights under the GDPR.[2]

5.1 The Right to be Informed (Privacy Notice)

Individuals have the right to know how their personal data is collected and used. Data Subjects are entitled to clear and straightforward information about how their data will be handled. The Privacy Notice available on VCAD's website outlines how the College collects, processes, and shares personal data, as well as the rights individuals have regarding their data.

[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/

Employees contractually agree to the processing of their personal data by VCAD as necessary for fulfilling their employment contracts and supporting the College's operations.

5.2 The Right to Subject Access (subject access request)

Individuals have the right to view and obtain a copy of their personal data and any other related information, and to confirm that their data is being processed lawfully and fairly. These requests must be directed to the Data Protection Officer, who will respond to valid requests within one month of receipt. This right does not extend to exam scripts or marks.

While individuals can access their personal data at no cost, the College may charge a reasonable fee to cover administrative expenses if:

- the request is clearly unfounded or excessive; or
- The individual asks for additional copies of their data after an initial request.

Further details about access rights and Subject Access Requests are available in the College's Data Subject Access Request Policy.

6. The Right to Rectification

Under the UK GDPR, Data Subjects have the right to request the correction of inaccurate personal data or the completion of incomplete data.

VCAD strives to maintain accurate records. If a Data Subject believes the College holds incorrect information about them, they may request a correction. The College will evaluate the request and make necessary amendments. In cases where data is incomplete, individuals may also ask for it to be completed or for a supplementary statement to be added.

These requests must be submitted to the Data Protection Officer, who will ensure a response is issued to valid requests within one month.

7. The Right to Erasure (the right to be forgotten)

UK GDPR grants individuals the right to request deletion of their personal data, though this right is limited and applies only in specific situations. It applies:

- when the data is no longer needed for its original purpose;
- when the individual withdraws consent; or
- when the data has been processed unlawfully.

This right does not apply if the data must be retained to:

- uphold freedom of expression and information;
- meet a legal obligation;
- perform a task in the public interest or under official authority;
- support archiving, scientific or historical research, or statistical analysis, where deletion would hinder the purpose;
- establish, exercise, or defend legal claims.

Requests for erasure must be directed to the Data Protection Officer, who will respond to valid requests within one month.

8. The Right to Restrict Processing

Data Subjects may request that the processing of their personal data be limited or suspended. This does not mean the data will be deleted, but that further processing will be restricted. This right is not absolute and applies only in certain cases:

- when the individual disputes the accuracy of their data and the College is verifying it;
- when the data has been processed unlawfully;
- when the data is no longer needed but must be retained for legal claims;
- when the individual has objected to processing and the College is assessing whether its legitimate interests override the objection.

9. The Right to Portability

This right allows Data Subjects to obtain and reuse their personal data across different services. It enables them to move, copy, or transfer their data from one IT system to another—such as to a different data controller—in a secure and user-friendly manner. It applies only to data provided by the individual or collected through their use of a service, such as online platforms like the College's Virtual Learning Environment. If technically feasible, the College will consider transferring the data directly to another organisation.

10. The Right to Object

Under the UK GDPR, individuals are entitled to object to the processing of their personal data under specific conditions. This includes the right to challenge certain types of processing, such as those carried out for direct marketing, research, or statistical analysis. The Data Subject must provide justification for their objection, except in cases involving direct marketing, where the right to object is unconditional.

11. Rights Related to Automated Decision-Making and Profiling

The UK GDPR includes rules regarding:

- decisions made entirely through automated processes without human input; and
- profiling, which involves automated analysis of personal data to assess aspects of an individual's behaviour or characteristics. Profiling may be used as part of automated decision-making.

Where automated decision-making or profiling could significantly impact Data Subjects, they have the right to request human review of the decision or to opt out of such processing altogether. These requests must be promptly directed to the Data Protection Officer.

These rights are not absolute and further details can be found through the Information Commission's Office (ICO).

When a Data Subject submits a request regarding any of the rights mentioned above, the College will evaluate the request in accordance with all applicable data protection laws and regulations. No fee will be charged for reviewing or fulfilling such requests unless they are considered excessive or clearly unnecessary. A formal response will be issued within 30 days of receiving the written request from the Data Subject. Verification procedures must confirm that the requester is either the Data Subject or their authorised legal representative.

12. Roles and Responsibilities

The **Data Protection Officer** (DPO) holds primary responsibility for ensuring compliance with data protection regulations. The DPO's duties are defined in Article 39 of the UK General Data Protection Regulation (UK GDPR), and they can be contacted at dpo_vcad@vcad.co.uk.

Each **Head of Division or Department** is accountable for ensuring that personal data within their area is processed in accordance with this Policy and any related rules, procedures, or guidance, and that staff have completed the required data protection training. They must also ensure that staff under their supervision implement suitable procedures, controls, and practices to comply with this policy.

All VCAD staff who handle personal data relating to students, employees, applicants, alumni, or other individuals must follow the rules set out in this policy. This includes:

- personal information is not disclosed by them either orally or in writing, to any unauthorised third party
- They do not access any personal data which is not necessary for carrying out their work
- Personal data in paper format is kept in a secure place when not being processed

- Personal data on computers should not be accessed or viewed by unauthorised staff or students, and as such, workstations must be locked or password-protected when not in use
- where personal data is held on paper, this should not be removed from the College
- staff processing personal data for research purposes should include a Data Protection Privacy Notice informing the data subject, in this case a research participant, of the following:
    - What data is being collected
    - Why the data is being collected
    - The legal basis for processing
    - How long will it be retained for
    - Rights of the participants
- Who to contact when they need to exercise their rights or complain as a participant. To complain about the research itself, the appropriate contact will be the team/person conducting the research. To enforce their rights, the contact is the Data Protection Officer dpo_vcad@vcad.co.uk.

Students may also need to collect and process personal data for academic projects or research, including surveys, interviews, and focus groups. In these cases, students are expected to follow the same responsibilities as staff.

Students must review the Privacy Notice available on the College's website and ensure that any personal information they provide to VCAD remains accurate and up to date.

When external organisations are contracted to process personal data on behalf of the College, VCAD retains full responsibility for ensuring the data is used appropriately and kept secure.

13. Data Sharing

Before implementing any new data sharing arrangement, it is vital to ensure compliance with data protection laws. This may involve conducting a Data Protection Impact Assessment (DPIA) to evaluate potential privacy risks and, if necessary, establishing a formal data-sharing agreement. The Information Commissioner's Office (ICO) offers a Data Sharing Code of Practice to help organisations share personal data in a lawful, fair, and transparent manner.

Personal data may also be shared internally within the College, provided there is a valid business reason, and the sharing complies with the principles of the UK GDPR.

When external organisations are engaged to process personal data on behalf of the College, VCAD remains responsible for ensuring the data is handled securely and appropriately.

Where a student requests that VCAD release their personal information to an external third party, the institution will do so only with the student's explicit consent. Students must complete the Consent to Share Information Form attached in Appendix D to authorise the disclosure and confirm the specific information to be shared.

14. Transfers of Personal Data Outside the UK

The UK GDPR limits the transfer of personal data outside the UK unless individuals' rights are protected or specific exceptions apply. Transfers are permitted to countries recognised under UK adequacy regulations, which include all EEA nations, as well as Andorra, Argentina, the Faroe Islands, Gibraltar, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, and South Korea.

Where personal data is transferred outside the UK to a country without an adequacy decision, VCAD uses an ICO-approved International Data Transfer Agreement (IDTA)

or the UK Addendum to the EU Standard Contractual Clauses (SCCs) and conducts a Transfer Risk Assessment.

15. Recordkeeping

Essential details such as names, course information, and contact details are recorded for administrative use. These records may exist in physical or digital formats and are used to arrange meetings, produce anonymised data reports, and enhance students' overall academic and personal experience. Any correspondence or documentation submitted by applicants or students may be linked to these records.

A designated senior manager is tasked with overseeing centralised recordkeeping to meet the expectations of students, the College, and relevant external organisations. For employee records, this responsibility is held by the Human Resources department.

To reduce redundancy and improve data protection, dedicated central systems like the Student Records System should be utilised. Any personal data stored in local databases—including those using reference codes instead of names—must be securely maintained.

The College is responsible for ensuring that all data remains accurate and current. Both staff and students must regularly update their personal details using the appropriate platform.

Sensitive data provided by applicants or students may be retained to offer suitable guidance or responses. Staff may share necessary information with colleagues or external parties when required to address concerns or support wellbeing.

Academic records—including grades, coursework, placements, and practical assessments—may be shared with authorised academic and administrative personnel and awarding organisations to validate results, determine academic progression, and issue qualifications.

In accordance with the UK General Data Protection Regulation (UK GDPR), the College must keep complete and accurate documentation of its data processing activities, including records of consent where applicable. These records must include:

- The name and contact details of the College as a Data Controller and the Data Protection Officer
- Clear descriptions of:
    - the personal data types we collect
    - the processing activities with which we engage
    - processing purposes
- Any third-party recipients of personal data
- Personal data storage locations
- Personal data transfers
- The retention schedule for personal data
- A description of the security measures in place for personal data including special categories of personal data.

The College is also required to document any incidents involving personal data breaches, including the context and the steps taken in response.

16. Confidentiality

Information received and recorded by VCAD is handled with care, discretion, and strict confidentiality. It is used solely for the purpose for which it was provided, and staff will not share personal data with third parties without the student's written consent, except in the following cases:

• When required by law, such as requests from courts, police, or other law enforcement bodies, or formal requests under the Data Protection Act

• When there are concerns about the welfare or safety of the individual or others

• When sharing anonymised statistical data that cannot be used to identify individuals

17. Data Retention and Disposal

VCAD is required under the Data Protection Act 2018 to retain personal data for operational needs while ensuring compliance with data protection principles. This includes adhering to the principle that personal data should not be kept longer than necessary.

Personal data must be retained only for as long as it serves its original purpose. This applies to data stored on central systems, personal computers, laptops, mobile devices, or in paper format. Once the data is no longer needed, it must be securely deleted or destroyed in accordance with the timelines established in the Retention Schedule.

VCAD will remove or destroy notes and records from its systems securely when there is no longer a legal, operational, or business need to retain them, based on the original reason for collection. All staff must consider safety and security when disposing of personal data during their duties. The sensitivity of the data and the format in which it is stored should also be considered.

18. Liaison and Correspondence

In some situations, staff may need to contact a third party on behalf of an applicant or student to address their concerns or questions. However, staff will only do so with written consent from the applicant or student, unless exceptional circumstances apply. If permission is given, the nature of the communication will be agreed upon beforehand. Staff will not share personal data without consent, except in emergencies or exceptional cases:

- When legally required to release information to authorities such as the Police, courts, Student Loan Companies, UK Visas and Immigration (UKVI), or other law enforcement agencies. A formal request under the Data Protection Act 2018 is typically required before releasing such information

- If the applicant or student is under 18 and there are serious concerns about their wellbeing
- If there are significant concerns that the applicant or student may pose a risk to themselves or others
- When sharing anonymised statistical data that cannot be used to identify individuals, which may be distributed across the College to identify trends and improve services

If staff are uncertain about whether they can legally share personal data, they should consult the Data Protection Officer at dpo_vcad@vcad.co.uk.

19. Students with a Disability, Longer-Term Medical Condition, or Specific Learning Difficulty

If a student has disclosed a disability, long-term health condition, or specific learning difficulty, VCAD is legally obligated under the UK's Equality Act 2010 to make reasonable accommodations to help the student fully engage with the educational opportunities offered by the College.

Information about the student will only be shared with their consent. If the student does not provide permission, this may significantly limit the extent and type of support VCAD can offer.

20. Data Breach Management

VCAD places a strong emphasis on staff training and individual accountability in complying with data protection laws.
While the College takes extensive precautions to prevent data protection breaches, occasional errors may still occur. Examples of incidents involving personal data include:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use

- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

All breaches of data protection should be reported to the Data Protection Officer as per the Data Breach Management Procedures. The Data Breach Incident Reporting Form included in that protocol must be completed with accurate and detailed information about the event, including the identity of the person reporting and the type of data affected. VCAD will assess all incidents promptly and notify the ICO within 72 hours of becoming aware of a notifiable personal data breach, in accordance with Article 33 of UK GDPR.

It is critical that staff report any breach or potential breach immediately. Prompt reporting enables swift action to contain the issue and ensures the College meets its legal obligation to report breaches.

If a breach of the Data Protection Policy is found to be due to clear negligence or deliberate action by staff or students, the College will assess the situation and determine appropriate next steps. In cases where a staff member is found negligent without valid justification, disciplinary action will be taken in accordance with the College's Staff Disciplinary Policy & Procedure. All factors will be taken into account when determining appropriate action, including whether the beach was reported promptly.

Once a breach has been reported, an initial review will be conducted to assess its seriousness. Serious breaches of data protection legislation may result in enforcement action by the Information Commissioner's Office (ICO), including administrative fines of up to £17.5 million or 4% of annual global turnover, whichever is higher, in accordance with UK GDPR.

21. Making a Complaint

VCAD is dedicated to managing personal data in line with legal requirements.

Concerns or complaints about the College's handling of personal data should be directed to the Data Protection Officer at: dpo_vcad@vcad.co.uk, which will be dealt with via the Student or Staff Complaints Policy & Procedure.

All Data Subjects have the right to make a complaint about our handling of personal data to the Information Commission's Office: https://ico.org.uk/make-a-complaint/.

22. Equality Statement

This policy reflects the provisions set out in the Equality Act 2010, which ensure no less favourable treatment based on protected characteristics and respect human rights.

23. Review of the Policy

This policy is reviewed every 18 months by the Senior Management Team and may be triggered by legislative changes.

24. Related Internal Policies and External Reference Points

Internal Policies

- Information Security Awareness Policy
- Retention Schedule
- Privacy Notice
- Cookie Policy
- CCTV Policy
- Data Subject Access Request Policy
- Data Breach Management Procedures
- Staff Disciplinary Policy & Procedures
- Student Disciplinary Policy

External Reference Point:

- Equality Act 2010
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)

Appendix A: Definitions

This section provides definitions and explanations of important terms related to data protection.

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an address, a student number, an IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data may also include special categories of personal data (see below). These are considered more sensitive and may only be processed in limited circumstances.
Special Category Data	Sensitive data that requires extra protection. Special category personal data relates to an individual's race, ethnicity, political opinion, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.
Anonymisation and Pseudonymisation	If personal data can be truly anonymised, then the anonymised data is not subject to data protection legislation. If this is not possible, it is advisable to aim for partial anonymisation or pseudonymisation of data. Pseudonymisation involves separating personal data from direct identifiers, so that no connection to an individual can be made without additional information held separately. Although partially anonymised and pseudonymised data are not exempt from data protection legislation, we recognise that they provide an added layer of security for the handling and processing of data.
The Data Controller	The individual/organisation registered with the Information Commission who is responsible for ensuring compliance with

	the requirements of the Data Protection Act 2018 and UK GDPR. This includes determining the purpose(s) for which personal data are collected and processed, and the means by which that data is processed. VCAD is the Data Controller.
Data Processors	Any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the Data Controller.
Data Protection Officer	The person appointed as such under the UK GDPR is responsible for advising the Institution (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the Institution's policies, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.
Processing	Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.
Data Protection Impact Assessment (DPIA)	It is a tool for identifying and reducing risks in processing activities.
Consent	It is the freely given, specific, informed, and unambiguous indication of a data subject's wishes for the processing of their personal data.
EEA	Refers to the 27 countries in the European Union, as well as Iceland, Liechtenstein, and Norway.
Data Subjects	An identifiable living person who can be identified, directly or indirectly, from personal data. This may include current, prospective and former staff or students, suppliers of goods and services, business associates, etc.

Appendix B: The Lawful Bases for Processing any Personal Data

The College must meet one or more of the following six legal bases to be able to process personal data:

- the data subject has given **consent** to the processing for one or more specific purposes. This consent must be provided by way of a positive action, and a record of consent must be maintained. It must be as easy for the subject to opt out as it was for them to opt in.
- processing is necessary for the performance of a **contract** or to take steps, at the request of the data subject, before entering into a contract; for example, processing carried out by the College to provide services to subjects, including staff and students.
- processing is necessary for compliance with a **legal obligation**. There must be a specific piece of legislation which requires the personal data to be processed.
- processing is necessary to protect the **vital interests** of an individual. This is mainly relevant in 'life or death' situations only.
- processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the College. The College may be able to rely on this for any activities carried out in the exercise of its public function, such as the retention of student transcripts and the management of staff.
- processing is necessary for the **legitimate interests** pursued by the College, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Due to its sensitive nature, the College must fulfil further conditions, in addition to the above, whenever Special Category Data is processed. These conditions are set out in the Data Protection Laws.

Appendix C: The Lawful Bases for Processing Special Categories of Personal Data

The lawful bases for processing special categories of data are set out in Article 9 of the UK GDPR and supplemented by conditions under the Data Protection Act 2018. When processing special categories of data, at least one condition from Article 6 and one from Article 10 of the UK GDPR must be met. These conditions include:

- The data subject has given explicit consent.
- The processing is necessary for employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests (either the data subject or another natural person) where the data subject is physically or legally incapable of giving consent.
- The processing is manifestly made public by the data subject.
- The processing is necessary for legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for medicine, the assessment of the working capacity of the employee, the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to certain safeguards.

Appendix D: Consent to Share Information Form

Student Details

Please fill in your full name, student ID, email address and phone number:

Authorised Third Party Details

Please fill in the full or organisation name of the authorised third party, their relationship to you and their contact information:

Data to be Shared

Please specify the personal data to be shared:

Purpose of Sharing

Please specify the purpose for which the data is being shared:

Consent Declaration

I, the undersigned, hereby authorise the university to share my personal data as specified above with the authorised third party. I understand the implications of sharing my data and consent to this action. Signature and Date:
