Information Management and Data Protection Policy

Policy Category:	Governance
Title:	Information management and data protection
Approving Authority:	Academic Board
Reviewed	January 2025
Effective Date:	31/01/2025

1 Introduction and Principles

1.1 At Results Consortium (hereafter 'the College') we are fully committed to protecting personal data and the collection, storage, disposal and use of personal data, in accordance with the General Data Protection Regulations (2018) and Data Protection Act (2018).

1.2 The purpose of the GDPR (2018) and Data Protection Act (2018) is to protect the rights and privacy of individuals, to ensure that personal data and information is not processed without their knowledge, and, is processed with a clear legal basis.

1.3 **The Six Principles** - We comply with the following six principles when processing personal data, always ensuring that it is:

- Collected and processed fairly, lawfully and transparently.
- Collected for a specific, explicit, legitimate purpose and used for that purpose only.
- Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
- Accurate and up to date.
- Kept securely, for no longer than is necessary for the purpose for which the personal data are processed, then disposed of securely.
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4 The College needs to process certain information about its staff, students and other individuals it has dealings with for operational purposes.

1.5 This policy applies to all students and staff (including visitors, partners contractors) at the College and the handling of all personal data processed by the College regardless of the form in which it is stored.

2 Roles and Responsibilities

2.1 Compliance with data protection legislation is the responsibility of ***all* staff members and students**, who must follow the six principles above and procedures below.

2.2 **Members of the College** (staff and students) are responsible for ensuring that any personal data they supply about themselves to the College are accurate and up to date.

2.3 The **Board of Governors** has ultimate responsibility for compliance with data protection legislation and must assure themselves that effective mechanisms are in place to protect personal data processed by the College.

2.4 The **Principal** is the **Data Protection Officer** and will:

2.4.1 keep the Board of Governors updated about responsibilities, risks and issues

2.4.2 provide information and guidance on processing data

2.4.3 promote a culture of understanding and compliance

2.4.4 monitor compliance with data protection legislation

2.4.5 advise on the necessity of Data Protection Impact Assessments and the manner of their implementation and outcomes

2.4.6 act as the organisational contact to the Information Commissioner's Office for all data protection issues, including breach reporting

2.4.7 maintain a log of incidents, remedial recommendations and actions

2.4.8 act as the contact for data subjects on privacy matters, including compliance with Subject Access Requests

2.5 The **Quality Manager** reviews and updates policies and procedures, making sure they are accessible.

2.6 **Human Resources**, in conjunction with **Line Managers**, encourage good practice when handling information, ensure that staff remain compliant with mandatory data protection training, and abide by this policy

3 Procedures

3.1 Accessing and processing data

3.1.1 Data may only be accessed by those with the authority to access it, and only for authorised purposes. Data must not be given to those without appropriate authority to access it.

3.1.2 Policies on computer access, password protection, cyber security and file naming conventions must always be complied with.

3.1.3 Devices containing personal data must not be removed from the College's premises unless appropriate security measures are in place, (secure log-in, password and authenticator app)

3.1.4 Care must be taken to ensure that computer monitors and device screens are not visible, except to authorised staff of the College.

3.1.5 Workstations must be secured when left unattended so no unauthorised person can access data.

3.2 **Storing, retention and disposal of data**

3.2.1 The following types of data will need to be retained to comply with the law and legitimate business needs. These include, but are not limited to:

Student data

- Applications
- Enrolment
- Attendance
- Achievement
- Progress tracking
- Academic records
- Assessment feedback and evidence
- References
- Post-course destinations

Staff data

- Contracts
- Tax and pension information
- Records of disputes or litigation
- Job applications, references and selection processes

3.2.2 All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access
- in a locked drawer or filing cabinet
- password protected, if computerised

3.2.3 Personal data must not be stored on local drives of PCs or laptops, or on personal devices used for work purposes (e.g. tablet or mobile phone).

3.2.4 Personal data must only be deleted or disposed of in line with the College's data retention guidelines.

3.2.5 Manual records that have reached their retention date are to be disposed of as 'confidential waste'.

3.3 **Data security and sharing**

3.3.1 Data must not, under any circumstances, be disclosed to a third party unless that third party has been specifically authorised by the College to

receive that information and has entered into a confidentiality or data sharing agreement.

3.3.2 The College ensures all third party organisations are able to offer assurances as to the systems and processes they have in place to ensure compliance with data protection legislation.

3.3.3 Where the College cannot identify a lawful basis for the sharing of data, the explicit consent of the data subject will be required for that particular purpose.

3.4 **Data breaches**

3.4.1 A data breach is a failure to keep data secure, which leads to the accidental or unlawful loss, destruction, alteration or unauthorised disclosure of that data.

3.4.2 Any concern about data being compromised in any way must be reported immediately to the Data Protection Officer (the Principal).

3.4.3 If anyone is concerned that any of the following has taken place, or is currently taking place, or is likely to take place, they must contact the Data Protection Officer (the Principal):

- Processing of personal data without a lawful basis
- Access to personal data without the proper authorisation
- Personal data not kept or deleted securely
- Removal of personal data, or devices containing personal data (or which can be used to access it), from the College's premises without appropriate security measures being in place

3.4.4 Certain breaches must be reported to the Information Commissioner's Office (ICO) and the Data Protection Officer will undertake an assessment of the likelihood and severity of any risk to people's rights and freedoms following the breach. Where this is found to be the case, the College is required to notify the ICO within 72 hours of discovering that the breach has taken place.

3.4.5 The main types of personal data breach are:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a member of staff 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 recipient, 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 an encryption key

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

3.4.6 The College takes the risk to security loss very seriously and adheres to the legal framework set down by the Information Commissioner's Office (ICO) and industry standards. The College has a Breach Management Procedure to be followed in the event of a data breach or suspected data breach to ensure the College responds and effectively manages any breach in line with data protection legislation.

3.4.7 Actions include:

Containment and recovery	Respond to the incident immediately, which includes a recovery plan and, where necessary, implement procedures for damage limitation.
Assessing the risks	Assess any risks associated with a breach, as these could affect any procedures after the breach has been contained. In particular, the College will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to re-occur.
Notification of breaches	Inform, if appropriate, about an information security breach: data subject; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
Evaluation and response	Investigate the cause of the breach and evaluate the effectiveness of any response made. Update policies and procedures accordingly.

POLICY DETAIL	
Document name:	Information Management and Data Protection Policy
Version Number:	V4
Date for Review:	January 2026
Author:	Catherine (Kate) Rossiter
Owner (if different):	Dominic Hammond
Compliance Measures:	Procedures and practice reviewed. Further guidance, six principles and more detailed procedures added. Job titles and postholders updated.
Related Procedures/ Committees	IT Acceptable Use Policy CPD Policy Disciplinary Procedures Capability Policy Code of Ethics Code of Conduct