FIR TREE COLLEGE

EDUCATION I TRAINING I LEARNING

Data Protection Policy

Document Control	
Date Reviewed:	27.11.24
Date to be Reviewed:	1.9.25

Contents

1. Introduction

Fir Tree College must process personal data to fulfil its obligations as an employer and education provider. The college is committed to ensuring that the personal data we process is done so in accordance with the high standards set by data protection law in the United Kingdom (UK). This policy outlines how we comply data protection law.

A key of useful data protection terms has been included at appendix 1.

2. Legal Framework

When processing personal data, the college comply with the following legislation:

- UK General Data Protection Regulation (UK-GDPR) 2021
- Data Protection Act (DPA) 2018

In addition to the key legislation defined above, the college follow the standards set by the Information Commissioners Office (ICO), the UK governing body for information management.

This policy is linked to the following documentation:

- Records Management Policy & Retention Schedule
- CCTV Policy
- Privacy Notices
- Safeguarding Policy

3. Scope

This policy applies to all personal data processed by the college along with any information processed by third-party Data Processors and Joint Data Controllers. For the purposes of this policy, personal data is any information relating to an identifiable individual that is held on a physical or electronic filing system.

This policy applies to those individuals whose personal data is processed by the college namely:

- Students (including prospective students)
- Parents & Guardians
- Staff (including applicants)
- Governors & Volunteers
- Contractors
- Visitors

4. Data Controller

The college is the 'Data Controller' for the personal data that we process which means that we are responsible for that data and make key decisions on how it is used. The college is registered with the ICO **(ZA075346)** and renews its subscription annually.

5. Data Protection Officer (DPO)

The college has appointed a Data Protection Officer (DPO) to oversee compliance with this policy and the aforementioned data protection legislation. Our DPO is Miss Danielle Eadie of RADCaT Ltd who is supported internally by the college's leadership team.

Our DPO acts as the first point of contact for the ICO and those individuals whose personal data is processed by the college. Our DPO can be contacted via the college office or directly using the following details if there are any questions about this policy or data protection in general:

DPO: Miss Danielle Eadie

A: RADCaT Ltd, 6 Seven Stars Road, Wigan, WN3 5AT

T: 01942 590 785 | e: Danielle.eadie@radcat.co.uk

6. Responsibilities

This policy applies to all staff employed by the college and those working with us on a temporary and / or voluntary basis. Third-party individuals or organisations contracted to process personal data on our behalf will be required to comply with this policy.

6.1: The Board of Governors

The Board of Governors have an overall responsibility for ensuring that the college complies with its data protection obligations.

6.2: College Senior Leadership Team (SLT)

The SLT are responsible for allocating the resources required to meet and maintain high standards of data protection compliance. The SLT will oversee and communicate the provisions of this policy to staff. In conjunction with the DPO and governing board where necessary, the senior leadership team will be responsible for making decisions regarding data processing.

6.3: All Staff

All staff (including temporary staff, volunteers and contractors) are responsible for processing personal data in accordance with this policy. Staff members that do not adhere to this policy may face disciplinary action.

The college ask that all staff contact the DPO without undue delay if the following situations:

- They have questions or concerns regarding this policy, data protection law, retaining personal data or how to keep information secure and confidential.
- There are concerns that this policy is not being followed.
- They wish to engage in a new activity that involves processing personal data.

- They are asked to share personal data with a third party.
- A data breach, near miss or gap in security has been identified.
- They receive a request regarding the rights of individuals such as requests for copies of personal data.

The college ask that all staff inform us in a timely manner if there are any changes to their own personal data such as address and contact details.

7. Data Protection Principles

The UK-GDPR sets out six key principles that the college must comply with to ensure personal data is secure and confidential. The UK-GDPR asks that personal data is:

7.1: Processed lawfully, fairly and in a transparent manner

Lawfulness:

The college will not process personal data unless it can meet **one** of the lawful bases (legal conditions) set out in Article 6 of the UK-GDPR. Personal data is processed:

- To comply with a **legal obligation**.
- To fulfil a **contractual obligation** with the individual.
- To perform a **public task**; the data is processed to perform a specific task in the public interest that is set out in law.
- To protect or save someone's life; there is a **vital interest**.
- To meet the **legitimate interests** of the data subject, college or another third party providing the processing is expected and does not impact the data subjects privacy too much.
- With the **consent** of the data subject (or their parent / guardian) in respect of children and vulnerable adults.

When processing special categories of personal data, the college will meet an additional lawful basis from Article 9 of the UK-GDPR and Data Protection Act. Special category data is personal information that is much more sensitive in nature and includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (fingerprints etc) if used for identification
- Health data
- Sex life and orientation

The lawful bases when processing such information will depend upon the purpose. Typically, the college will rely upon one of the following:

- Special category data is being processed in the field of **employment, social security and social protection.**
- The college has deemed there is a **substantial public interest** to process the special category data.

- The individual has provided their **explicit consent** (written) permitting the college to process their special category data.

Fairness and Transparency:

Prior to the processing of any personal data, the college will inform individuals how and why their personal data will be used by issuing privacy information.

Consent

Where consent is the lawful basis relied upon for the processing of personal data, the college will ensure that the individual:

- Has a clear understanding of what they are consenting to and why; it is informed.
- Understand that the use of their personal data is optional.
- Is given clear instruction on how they can withdraw their consent or change their preferences.

The college issue consent forms as part of its admissions pack for routine data processing activities that are optional; a log of consenting and non-consenting students is kept. Consent based activities for staff are much less frequent with permission sought on an ad-hoc basis.

Consent & Students

The college understand that student personal data belongs to them and not their parent or guardian. However, some students have certain vulnerabilities that may impact their ability to understand and make decisions about their own data. In such cases, the college will obtain consent from their parent or guardian.

The college will assess consent on a case-by-case basis.

Consent & Safeguarding Referrals

In instances where the college has a significant safeguarding concern about an individual, consent will not be sought to make a referral to the police or social services unless it is appropriate to do so. Data protection law provides provisions to ensure data can be shared with the right people at the right time in the event that someone is at risk of harm. Please refer to the 'Safeguarding Policy' for more information.

7.2: Collected for specified, explicit and legitimate purposes only (purpose limitation)

The college will not process personal data unless there is a valid purpose for doing so, nor will we use data for a new purpose without informing individuals and ensuring compliance with the key GDPR principles. The college will explain the reasonings for processing to individuals at the point of collating their personal information.

Staff within the college should not process personal data for any new purposes outside of their approved duties without permission; immediate management and the DPO should be consulted where necessary.

7.3: Adequate, relevant and limited to what is necessary (data minimisation)

The college will only process the minimum amount of data necessary to fulfil the purposes for which it was collected. Data collection forms and platforms are carefully designed to ensure only categories of data that are strictly necessary will be inputted to ensure staff and individuals do not provide any

excess data. The college adopt a minimalist approach to data processing and prompt staff to always question what is absolutely necessary.

Special categories of personal data should only be shared or processed if it is absolutely necessary; staff should seek approval if there are any concerns or doubts.

7.4: Accurate, up to date and complete (data accuracy)

The college make reasonable attempts to ensure personal data is up to date and accurate. Checks are performed at least annually to ensure basic student and staff data such as contact details are accurate.

The college has implemented information management systems that integrate with other key software meaning that changes to data are automatically updated across the board.

Meeting notes and key records are reviewed by relevant parties prior to finalising to ensure a uniform agreement to the content. Staff are encouraged to keep records factual and succinct.

If reasonable attempts to rectify incorrect information are not possible, the college will ensure records are securely deleted.

7.5: Kept only as long as necessary to meet the purpose for processing (storage limitation)

Personal data will only be kept for as long as necessary to fulfil the purposes for which it was collected; records will not be kept 'just in case' they may be needed in future.

The college has implemented a 'Records Management Policy and Retention Schedule' that provides guidance on how long personal data should be kept and the approach taken by the college to manage those records in line with data protection legislation.

The college perform a review of records at least annually to ensure that any records no longer required are securely disposed of. Automated deletion should be applied where necessary for any electronic records that do not require a manual review.

7.6: Processed in a manner that ensures its integrity, security, and confidentiality.

The college must ensure that adequate control measures are in place to protect the integrity and confidentiality of the personal data that we process in both physical and electronic formats. Security is a vital element in our approach to data protection and high standards are achieved by the following key control methods:

- Ensuring a clear desk at all times; documents and data storing devices such as laptops, mobile phones and tablets should not be left unattended; routine walkaround checks are made to assess compliance.
- Physical records and devices to be kept in locked cabinets with key access strictly limited.
- Auto lock activated on all devices and screens locked if a staff member leaves their workspace.
- A full and up to date asset and software register to map out where data is stored that includes a log of devices / records that are taken off site.
- Access controls in place on all records to ensure staff only access the records they need to perform their roles.
- User accounts and devices issued to individual staff members will not be shared with other users.
- Passwords changed on a routine basis and must contain a combination of letters, numbers and special characters; multi-factor authentication will be utilised where available.

- A process to ensure all visitors to site are effectively managed and not permitted entry without an ID badge and DBS checks where necessary.
- Staff receive routine training on data protection and security, sign confidentiality and acceptable use agreements and partake in DBS checks.
- Access to records and user accounts is to be removed without undue delay if a staff member leaves their employment; an exit checklist is in place.
- Compliance checks and 'Data Protection Impact Assessments' (DPIA) where necessary performed on data processing suppliers.

The college monitor compliance checks with the above control measures by performing regular audits on security which includes:

- Routine walkaround checks on a departmental level to identify any areas of non-compliance.
- Annual audit performed by the DPO to assess the college's compliance with the principles of the UK-GDPR; a report will be provided.
- Regular gap analysis and monitoring on college systems performed by the ICT department(s) to highlight any gaps in security.
- External audits performed at intervals.

7.7: Accountability

Accountability is the overarching principle of the UK-GDPR and requires the college to demonstrate how it complies with the six core principles. The college achieve accountability by:

- Implementing key data protection policies and procedures and communicating these with staff and other relevant parties.
- Applying the core data protection principles in other key operational areas of the college namely; HR, Marketing, Finance, Health & Safety and Safeguarding.
- Keeping adequate logs of data breaches and reviewing logs on an annual basis to assess areas for improvement.
- Keeping records of consent, requests regarding the rights of individuals and decision making.
- Keeping a 'record of processing activities' that clearly outlines an up-to-date inventory of data, the purposes and lawful bases for processing and key characteristics regarding how that data is managed.
- Implementing data sharing agreements and compliance checks on third party Data Processors and Joint Controllers.
- Completing 'Data Protection Impact Assessments' where necessary on any high-risk data processing areas.

8. Data Sharing

The college must share personal data to meet its legal and operational obligations as an employer and education provider. Routine data sharing is limited to the following:

- Statutory data collections submitted to the Local Authority and Department for Education.
- Transfers of records between educational settings that students attend.
- Transfers of data to and from the government to meet a legal obligation (HMRC, Funding etc)

- Liaising with or making referrals to third party agencies when additional support for staff or a student is required.
- Sharing data with our suppliers and providers of professional services if it is required to fulfil their services to us (IT, Payroll, Legal Advisors etc)

In certain circumstances, the college must share personal data with law enforcement, governing bodies and legal entities when required to do so to including:

- In the prevention and detection of crime and to apprehend offenders.
- In connection with legal proceedings and claims.
- A significant safeguarding concern has been identified.
- Supporting the emergency services if an accident or incident has occurred.
- Supporting an investigation.

When sharing information with third parties, the college will:

- Implement data sharing agreements that clearly outline the expectations and responsibilities of each party.
- Only share information with third party providers of services if they can guarantee that they comply with data protection law and high standards of security.
- Limit the personal data shared to what is absolutely necessary to fulfil the purpose of the data transfer.
- Keep a log of compliance documentation including data sharing agreements, privacy notices and security questionnaires.
- Complete DPIA's on any data transfers that pose a high risk the rights and freedoms of individuals.

The college ask that staff do not share personal data unless the transfer has been approved by their senior management with support from the DPO where necessary.

In respect of any personal data that is transferred outside of the United Kingdom, the college will ensure appropriate safeguards are in place that comply with data protection legislation. The DPO should be consulted for all transfers of data internationally.

9. The Rights of Individuals

The UK-GDPR sets out 8 rights for Data Subjects that the college must comply with in certain circumstances:

9.1: The Right to be Informed

The college will issue 'Privacy Notices' to all parties whose data we process. Privacy Notices are issued at the start of our relationship with individuals to inform them what data we will collect, how it used and why we need it. We ensure that Privacy Notices are displayed in accessible locations for each party should they need to access them:

Data Subjects	Privacy Notice Issued:	Location
Students, parents & guardians	In admissions pack	Website

Applicants	With application form (a link directing applicants to the relevant website section may be preferable)	Website
Staff	In induction pack	Staff Handbook or Shared Staff Policy Area.
Governors & volunteers	In induction pack	Shared Gov / Volunteer Policy Area.
Visitors	Notice in reception about where privacy information can be found.	Website and printable copies available at reception.

All college privacy notices will include the following:

- The name and contact details of the college as Data Controller
- The name and contact details of the DPO.
- The categories of personal data being processed.
- How the information was obtained and whether processing is optional or compulsory
- The purposes for processing the data.
- The lawful bases for processing (including special categories of personal data)
- The recipients of personal data if shared with third parties.
- Details if personal data is shared outside of the United Kingdom
- Retention periods for the personal data
- The rights available to the individual
- The right to withdraw consent where applicable.
- The right to complain to the college and ICO (include instructions)

Privacy Notices are reviewed on an annual basis or sooner should a change in legislation or data processing activities occur.

9.2: The Right of Access

Individuals have a right to request access to the personal data that the college holds about them, this is referred to as a 'Subject Access Request'.

The college ask that requests are made in writing and include the individuals name, contact details and specific details regarding the records they are looking to access. Requests should be sent directly to the college office who will liaise with the DPO to process the request. The DPO will be informed without undue delay if a request is received.

The college will assess the request to establish whether any of the following are required:

- Proof of identity if there is any doubt the requester is who they say they are.
- Proof of parental responsibility if the request relates to a child or vulnerable adult and there is uncertainty that the individual has legal right to act on their behalf.
- Letter of authority if the request is made by a solicitor on behalf of a client.

The college will provide an email confirming receipt of the request informing the individual that a response will be provided within one calendar month from the date the request was received. Please

note that if additional information is required from the individual (consent, ID etc), the one calendar month response time will only commence once the college is satisfied the request has been verified.

A response to all requests to access personal data should be provided within one calendar month informing the requester that:

1. The request has been met in full with the relevant information enclosed.
2. The college has deemed that the request is complex and will exercise the right to extend the response time by a further two calendar months (three months in total)
3. The request has been denied, including the reasons why.

All responses will be accompanied by a letter or email from the college that includes:

- Details of the information that has been provided.
- Details of any information that could not be provided (if any) and the reasons why.
- A copy of the relevant Privacy Notice or reference to where it can be located to ensure the requester clearly understands how and why their data is processed.
- Information on how the individual can raise a complaint to the college and / or the ICO if they are unhappy with how their request has been handled.

Requests unless otherwise stated will be provided in electronic format with password protection in place. A proof of receipt should be sought.

Exemptions

A number of exemptions are provided in the Data Protection Act to cover scenarios when it may be inappropriate to disclose personal data as part of an information request. For example, if disclosure could cause serious harm to the individual or a third party.

The college will consult the DPO prior to providing any information if there are any concerns at all that disclosing the requested data could cause harm to the individual or another party.

Redactions

The college can only provide the individual with information about themselves and not that of any third parties without their consent unless we deem it reasonable to do so. Redactions to third party data will be applied where necessary.

In the case of student records, it is generally accepted that the identities of college staff, social workers and health professionals remain visible. Records must however be reviewed on a case-by-case basis.

In situations where it is impossible to separate the individual's data from that of another person, the information may be omitted. The DPO will be consulted if there are any concerns regarding redactions.

A log of all information requests will be kept on the colleges 'information request register'.

9.3: Right to Rectification

Reasonable attempts will be made by the college to ensure personal data is kept up to date and accurate. A check (at least annually) will be made to ensure basic identifiers and contact information is up to date; this will include details of emergency contacts.

Regular correspondence is made, and logs kept regarding allergies, medication and any special educational needs or health requirements to ensure it is up to date.

Any data processing activities relying upon consent will be reviewed on an annual basis; consent will not be assumed.

Requests made to update basic information such as name changes and contact details will typically be fulfilled straight away by college staff. In situations where an individual makes a request to have more complex data rectified such as meeting notes, health and safeguarding records a review will be required with input from the SLT and DPO.

9.4: Right to Erasure

The right to erasure will only apply in certain circumstances as the college has legal and operational obligations to retain data. The right to erasure will apply in the following circumstances:

- consent is the lawful basis for processing; the individual has a choice.
- the data is no longer necessary for the purpose in which it was collected.
- the processing is determined to be unlawful.
- there is a legal obligation to remove the data.

In such circumstances, the college will securely dispose of the personal data in question and a confirmation will be provided to the individual.

In the event that a request to be forgotten cannot be met, the individual will be provided with an explanation which includes the set retention period for their personal information.

9.5: Right to Restrict Processing

The right to restrict processing is not an absolute right and will only apply in the following situations:

- The individual contests the accuracy of their personal data.
- The individual challenges the college's lawful basis for processing their data.
- The college no longer needs the data but the individual asks that we retain their records for the establishment, exercise or defence of a legal claim. The college will continue to store the data but will not process it any further.
- The lawful basis is legitimate interests, and the individual feels their own interests are being overridden by the processing.

The college will refrain from processing for a temporary period whilst a review into the individuals request is reviewed.

Individuals will be provided with an outcome of their request that includes details on whether or not processing will continue along with the reasons why.

9.6: Right to Object to Processing

There are three main instances in which individuals have a right to object to the processing of their personal data:

- The processing of personal data is for the purposes of direct marketing; the processing is therefore optional.
- Personal data is being processed for scientific, historic or statistical research purposes unless the processing is necessary for the performance of a task in the public interest.
- The lawful basis for processing is for the performance of a task in the interest of the public or legitimate interests.

Where the processing of personal data is optional, the college will remove the individual's data if an objection request is received.

The college do not process personal data for research purposes unless it is strictly necessary for the performance of a task in the public interest. We will however review such requests and provide an explanation to the individual if their request cannot be met.

Should the lawful basis for the data in question be public task or legitimate interests, the college must demonstrate compelling grounds to continue processing following receipt of an objection request. The college must justify why the processing overrides the individuals' own interests.

9.7: Data Portability

The college understand that individuals have a right to ask that any data they provide to us is transferred from one IT environment to another by automated means between Data Controllers. It is not anticipated that there are any instances in which this right would currently apply to the colleges processing of personal data, we will however review any requests with the DPO.

9.8: Automated Decision Making & Profiling

The college do not currently partake in any data processing based upon automated decision making and profiling.

9.9: Responding to Data Subject Rights

The college will respond to all requests regarding data subject rights within one calendar month; the college reserve the right to apply a two-month extension for any requests that we deem complex, we will however inform the individual of any intention to extend within the first month.

All responses should confirm whether the college has been able to meet the request in full, part or not at all along with a clear explanation why. A copy of the relevant privacy notice will be included or referred to in all responses; the individual will also be informed of their right to complain to the ICO if they are unhappy with how the college has dealt with their request.

9.10: Recording the Rights of Individuals

To meet the UK-GDPR's accountability principle, the college will retain a log of all requests received regarding the rights of individuals. The log will include:

- Name & contact details of requester
- Date of request
- Whether the identity of the individual has been verified
- What has been requested
- Whether the request has been met in full, part or refused and the reasons why.
- Date of response.

Logs will typically be kept for a period of one year to account for the complaints process.

10. CCTV

Closed Circuit Television (CCTV) is in place at various location across the college site to enhance security and aid in the prevention and detection of crime. The college comply with the ICO code of practice for the use of CCTV, in summary:

- A lawful basis for the use of CCTV has been established.
- DPIA's will be conducted and reviewed routinely to determine the privacy risks associated with the use of CCTV.
- Prominent signage will be placed at key areas that clearly informs individuals that CCTV is in place, the reasons why and details of the Data Controller.
- Access to the system is strictly limited to the designated staff member(s) identified in the DPIA; password protection is in place to restrict access to unauthorised users.
- Footage will not be released to individuals or third-party organisations such as the Police or Insurers without written authorisation from the headteacher and consultation with the DPO.

Please refer to the college CCTV Policy for further information.

11. Images

From time to time, we use images to celebrate achievements, promote the college and provide the community with an insight into college life; images also provide students and families with mementoes of their time at college. For the purposes of this policy, images refer to photographs and video footage processed by the college.

The use of images will typically be limited to the following:

- Internal displays
- Our website(s)
- Social media
- Local media (newspapers etc)
- Newsletters and circulars
- College photographers (annual photographs for parents)

The use of images for such purposes is optional and therefore consent will be sought prior to any images being taken or used. Consent will be sought in line with the process outlined in section 7 of this policy.

The college adopt the following approach:

- Staff will be provided with a log of consent which will be reviewed prior to images of students being taken.
- Images will not be accompanied by any further identifying features such as a full name unless explicit consent is in place.
- Alternative provisions will be available where possible to ensure non-consenting students are not discriminated against and feel included.

- Particular attention is given to students and staff whose identities should not be made public for safeguarding purposes prior to publicising any images. Please refer to the college Safeguarding Policy for further information.
- Images will be taken on college owned devices only; personal devices will not be used.

12. Data Protection by Design & Default

In order to achieve an effective data protection strategy, the college must integrate the key principles of the UK-GDPR into its organisational culture, structure and core business functions. To do this, the college will consider the privacy impacts and risks associated with processing prior to any data processing taking place (data protection by design):

- Ensuring a legitimate purpose has been established and a lawful basis met.
- Assessing what data is required and how we can best limit this to what is strictly necessary.
- Completing a DPIA on any high-risk processing activities or new technologies.
- Exploring less intrusive methods of processing.
- Using anonymisation and pseudonymisation where appropriate.

The college will take a proactive approach to ensure data protection lies at the heart of our organisation and remains ingrained within our culture (data protection by default):

- Appointing a DPO to oversee compliance; regular updates are provided to college leadership.
- Performing routine audits on both physical and technical security measures to identify any gaps in compliance and security.
- Integrating data protection into key policies and procedures and effectively communicating these with staff.
- Regularly training and briefing our staff on data protection and associated topics including cyber security to keep privacy and security relevant.
- Promoting transparency and an open culture to ensure staff are not afraid to report data breaches or notify us if they have concerns.
- Displaying visual aids around site as reminders of the key principles.
- Reviewing key documentation at intervals to ensure the content and our practices complement one another and comply with the relevant legislation.
-

13. Data Breach Procedure

The college implement robust security measures to ensure as much as possible that data breaches do not occur. We do however realise that even the most secure of systems are not watertight, we have therefore implemented a procedure to help us deal with data breaches quickly and efficiently. In the unlikely event of a data breach, the college will follow the procedure set out below:

Notification

Upon discovering a data breach, staff will notify the college Data Protection Officer (DPO) without undue delay. Data Processors and Joint Data Controllers must also notify the college DPO of data breaches affecting college data.

Timing is of the essence; the sooner the college is notified of the breach the quicker we can work to mitigate the impacts. In addition, the college has a duty to report certain data breaches to the ICO within 72hours. We may also need to notify the affected individuals.

A list of key contacts will be readily available to staff to ensure the relevant person(s) can be contacted as soon as possible. Emergency contacts for the following individuals will be accessible:

- Data Protection Officer (DPO)
- Individual Responsible for Data Protection in the College
- ICT Lead (Cyber Related Breaches)

The college will keep contact details of the relevant department at the local authority and police should a significant data breach occur.

It is recommended that colleges add contact details for the relevant departments at their respective local authority and policing services should a significant data breach occur.

Assessment & Review

The DPO will investigate the report to determine whether a data breach has occurred and advise the college on the immediate steps required to mitigate the breach. Steps will differ depending upon the nature of the breach.

An assessment will then be made by the DPO to ascertain the likely impacts of the breach, the severity of those impacts and the likelihood that they will occur. The DPO will discuss the assessment with the leadership team at the college or relevant college and a decision made on reporting.

Reporting

Any data breach that is likely to result in a high risk to an individual's rights and freedoms will be reported to the ICO within 72hours of discovery using the following link: https://ico.org.uk/for-organisations/report-a-breach/

If the full details are not yet known, the DPO will provide as much detail as possible to the ICO within the 72hour window. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The college must also inform the affected individuals if there is a high risk to their rights and freedoms for instance if the breach is likely to lead to material, physical or mental harm. Individuals will be provided with an overview of the breach in writing, correspondence via telephone will be required for urgent situations. In addition to an overview of the breach, individuals will be provided with:

- The name and contact details of the DPO.
- A list of actions that have been taken to mitigate the breach and the adverse effects on them.
- Details on how to make a complaint to the ICO.

The college will consider support for the affected individuals where appropriate such as police involvement if the breach poses a threat to safety.

Data breaches that do not pose a high risk to an individual's rights and freedoms will be managed internally by the college.

The college will report significant cyber breaches to the National Cyber Security Centre (NCSC) and seek technical assistance from them where necessary: https://report.ncsc.gov.uk/

Recording

All data breaches no matter the severity will be kept on the college's data breach log which includes:

- Breach reference number
- Date of breach
- Staff member responsible
- No of individuals affected.
- Description of breach
- How it was discovered
- Categories of data affected.
- Potential consequences
- Actions taken.
- Whether it is reportable to the ICO and affected individuals (including dates reported)

The college encourage the reporting and logging of near misses to improve security measures.

The DPO will also record the assessment and decision-making process for high-risk reportable breaches.

Review

Once the college has taken the necessary actions to mitigate the breach as much as possible, measures to prevent the breach re-occurring will be discussed and implemented by the DPO and relevant staff members at the college.

The college will take steps to review and monitor the impact of the breach moving forward. This may include online searches to ensure data has not been publicised and corresponding with the affected individuals to monitor any impacts of the breach.

College staff will support the DPO where necessary throughout the data breach procedure.

14. Storage of Records

The college will store records securely and in an organised manner taking into account the following:

- Records need to be secure, yet accessible for use by the relevant staff members. Access controls must be in place to ensure staff only access what they need to.
- Records need to be searchable to ensure information requests can be met efficiently; a uniform method of addressing individuals is recommended to ensure records can be easily collated upon request.

- Records must be stored in chronological order to support their retention period; records ready for deletion should be identifiable.
- Staff are encouraged not to use their email account as a system for storage; key records should be filed on recommended databases only.
- The location of records should be known and logged for traceability; if a staff member leaves, the departmental lead will need to make records accessible to their replacement.

15. Disposal of Records

Once records are due to come to the end of their retention period, a review will take place to assess whether or not records are still required or if they can be securely destroyed. Particular care should be taken to review safeguarding and personnel files to account for any ongoing or likely investigations and claims.

Electronic records will be securely deleted from the college server and remote platforms taking into consideration any recycle bins and temporary deletion folders. Automated deletion will be applied for any electronic records that do not require a manual review prior to disposal. College ICT departments will be consulted to ensure records are fully cleansed and removed from the system(s).

Physical records will be securely shredded on site by college staff or via carefully selected shredding partners who provide adequate proof of destruction.

A general log will be kept outlining when data sets have been destroyed.

16. Training

All staff are subject to a data protection briefing upon induction and receive routine training on both data protection and cyber security. The college will issue staff with routine briefings at intervals to ensure the key data protection principles remain relevant.

Data protection will form a key part of staff continual professional development; a record of all training is kept by the college.

17. Monitoring

This policy will be reviewed every **three years** or sooner should a significant change in legislation or data processing activities occur. The Data Protection Policy is a statutory policy that should be reviewed by the governing board.

The policy and any changes will be communicated to all college staff.

Appendix 1: Useful Data Protection Terms

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Biometric Data	The automated recognition of individuals based on their biological and behavioural characteristics; examples include fingerprint and facial recognition scanning.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Information Commissioners Office (ICO)	Governing Body for data protection in the UK.
Data Protection Officer (DPO)	Appointed individual that oversees the colleges compliance with data protection law.