gloucestershire college

Quality Controlled Document

Policy: **Data Protection and IT Security** **Date:** **May 2019**

Approved by: **Principal and Chief Executive**

Contents:

Quality Controlled Document **POL - 04**

Policy: **Data Protection and IT Security** **Date:** **May 2019**

1. Introduction and Data Protection Principles

Gloucestershire College needs to collect and use information about people with whom it works. This includes information about our employees, students, applicants and parents/guardians of students; as well as details about people working in businesses. The College uses information to enable the fulfilment of contractual agreements with government funding bodies, carrying out its public task to provide educational services. As an employer, it is also necessary for the College to process information to monitor and enable staff recruitment and the fulfilment of related contractual agreements; and to market services to interested parties.

This policy sets out the College's obligations under Data Protection Legislation (see Appendix A for definition). It applies to all students, staff and other individuals about whom the College may hold personal data or who may process personal data held on behalf of the College.

All personal information must be processed in line with the data protection principles as set out in Data Protection Legislation.

In summary, these state that personal data shall be:

i. Processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
ii. Processed fairly and lawfully in a transparent manner
iii. Processed for one or more specified, explicit and legitimate purposes
iv. Adequate, relevant and limited to what is necessary.
v. Accurate and where necessary, kept up-to-date
vi. Kept in a form that permits identification of data subject for no longer than is necessary.
vii.

Data protection terms commonly used in this policy are listed and explained in **Appendix A.**

2. Categorisation of Data

Data in the College is categorised according to the following definitions:

2.1 **Personal Data** - Any information relating to an identified or identifiable natural personal. This can be direct or indirect identification and is technologically neutral.

2.2 **Sensitive Personal Data** – relates to one of the following:

- Racial or ethnic origin
- Political beliefs

- Religious or philosophical beliefs
- Trade Union membership
- Genetic or biometric data
- Physical or mental health
- Sex life or sexual orientation
- Criminal Records
-

2.3 Non-Personal Data – all other data.

Non-personal data can be either confidential or non-confidential information. Confidential information consists of information that, if disclosed or made public, could damage the College's commercial, financial interests or reputation; or cause the College to not meet its legal obligations. The definition of "confidential" includes any information that either is labelled as "confidential" or, if not labelled "confidential", would nevertheless be reasonably regarded as confidential.

3. Roles and Responsibilities

The College as a corporate body is the 'Data Controller', in that it determines the need to collect personal data and the uses to which it will be put. Responsibility for the overall management of the implementation of the relevant data protection legislation lies with the Principal, who vests day-to-day responsibility for implementing the provisions of this policy with the College's Data Protection Officer.

In some circumstances, the College contracts with third parties to process personal data on its behalf. These 'data processors' must provide sufficient guarantees to the College that measures are in place to ensure compliance with Data Protection Legislation. This will be determined through procurement procedures and subsequently, as contracts are put in place and monitored.

The College has identified clear roles and responsibilities with regard to protecting personal data and demonstrating the application of the College's data protection principles. The Director of HR should ensure that these roles and responsibilities are communicated to all new staff during induction. All managers are responsible for subsequently updating their teams, as well as monitoring and reporting performance during reviews.

3.1 Data Protection Officer

The College Data Protection Officer (DPO) is assigned on the basis of professional qualities and expert knowledge of the data protection law and practices, combined with knowledge of the further education sector, the College and its administrative procedures. The DPO plays a key role in fostering a data protection culture in the College and will provide advice on the interpretation and implementation of data protection controls and measures to ensure compliance with relevant legislation. The contact details of the DPO will be published to enable easy contact by post, by telephone or via a dedicated email address. The DPO should be involved properly, proportionately and in a timely manner in matters relating to the protection of personal data. The DPO will not be instructed in how to exercise their tasks and will be able to perform duties and tasks in an independent manner, having direct access to the College's senior level of management.

3.2 All staff

All staff have a responsibility to check that any information they provide to the College in connection with their employment is accurate and up-to-date and that they inform the College of any errors or changes.

The College encourages staff to raise questions about data protection matters and to report any issues or data breaches that they may come across in their work. Failure to follow the College's data protection principles as specified in this policy may result in disciplinary action being taken against the relevant member of staff.

All volunteers engaged by the College have the same responsibilities.

3.3 All Managers

All College managers have a responsibility to ensure their staff are aware of the College's Data Protection and IT Security Policy and associated procedures, and to know how to correctly process personal and sensitive personal data as part of their work. They should ensure that all staff have attended College induction sessions and mandated data protection training. All managers have a responsibility to ensure that any personal data breaches are reported to the College's Data Protection Officer within a timescale to ensure that the College's legal obligations to notify the Information Commissioner's Office (ICO) within 72 hours, is not put at risk.

Managers involved in the development, design or implementation of new systems or procedures in their work areas should contribute to, or lead on, Data Protection Impact Assessments aimed at reducing any risks to the safety or security of personal data. Managers may also be required to contribute to the completion of the Personal Data or Technical Security Registers as they apply to their work area.

3.4 Asset Owners

Additional responsibilities for managers who are identified as 'Asset Owners' include completion and maintenance of an accurate Personal Data Register for their identified work area and completion of associated regular risk assessments for the safety and security of personal data; the latter inform the Asset Owner of the need to implement technical and organisational measures to reduce any identified risks.

The Head of Data Management will maintain an accurate and up to date record of the named Asset Owners for the work areas in the College.

3.5 All students

All students should provide personal data as required by the College to fulfil its public task to provide educational services. Students have a responsibility to keep this up to date and inform the College of any changes.

4. Records

4.1 Personal Data Register

The College will keep records of personal data processing activities, in the form of a Personal Data Register. “Asset Owners” will be identified as being responsible for recording such activities in their work areas, along with the controls that are in place to safeguard the security and safety of that personal data. The College’s Data Protection Officer will review and combine entries to form the College Personal Data Register. The College Personal Data Register is available to the appropriate regulatory body - the Information Commissioner’s Office (ICO).

4.2 Technical Security Register

Director IT & Estates must maintain a Technical Security Register (TSR). This will identify the technical measures applied by the College to protect the security of the College’s network, systems and data. This could include, but is not limited to, network security, the prevention of malware and removable media risks, ensuring secure configuration, the appropriate use of privileges and access controls, cloud computing security, off site working arrangements and individual system specific technical security measures. The TSR will not be widely published but will be available as appropriate.

4.3 Other Data Protection Records

The College’s Data Protection Officer must keep the following records.

- The number, processing timescales and nature of Subject Access Requests, along with all correspondence.
- The number, processing timescales and nature of any other requests relating to individual rights as covered in the GDPR.
- The number, nature and related timescales of identified data breaches, supplemented with details of consequent investigations, recommendations and audits.
- Copies of Data Protection Impact Assessments, and related audits.
- Full detail of any communications with the Information Commissioner’s Office
- All reports and analysis related to personal data protection that are provided to the College Executive Team or Governors.
- Main Privacy Notice content and applicable dates.

Asset Owners must keep the following records in relation to their work areas:

- Records of access rights or permissions that are relevant to processing or systems in their work area.
- Records demonstrating consideration and focus on data protection in their work area.
- Records of supplementary Privacy Notices published and/or communicated verbally which relate to data processing in their work areas, including the applicable dates
- Records of any ‘consent’ collected from individuals, which relates to data processing and the applicable dates.
- Personal Data Register (PDR) content relating to their work area.

5. Fair and Lawful Processing

Personal data should be processed by the College in a lawful, fair and transparent manner.

5.1 Legal Bases

The College will identify the legal basis for processing personal data in the PDR. Article 6 of GDPR identifies the options as follows:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the data subject is party
c) Processing is necessary for compliance with the College's legal obligation
d) Processing is necessary in order to protect the vital interests of the data subject or other person;
e) Processing is necessary for the performance of a task carried out in the public interest;
f) Processing is necessary for the purposes of the legitimate interests pursued by the College

Point (f) will not apply where the College is carrying out tasks in relation to its role as a public body.

5.2 Transfer of personal data

The College does not transfer personal data outside of the European Economic Area.

5.3 Use of Consent as legal basis for processing personal data

Where consent is identified as the legal basis for processing personal data, the College will ensure that evidence is available to demonstrate that consent has been given. In all cases when consent is requested this will be in an intelligible and easily accessible form, using clear and plain language. An individual will be given opportunities to withdraw consent and College processes and systems will make this possible.

Where consent is the legal basis for processing personal data, this must be collected via a clear affirmative act, being freely given, specific, informed and an unambiguous indication of the individual's agreement to processing related to him or her.

5.4 Marketing Communications

Marketing communications and campaigns should be undertaken in line with Data Protection Legislation, and the Privacy & Electronic Communication Regulation (PECR). College staff should comply with PECR when making calls or sending texts or emails to generate marketing leads. Any calls texts or emails generated for direct marketing purposes are covered under the PECR.

Where College marketing activities, rely on 'consent' as the legal basis for processing personal data, the Head of Marketing must ensure that individuals have a genuine choice over whether or not to give their consent to communications. The College will not coerce, or unduly incentivize an individual to give consent, or penalize anyone who refuses.

5.5 Use of CCTV

At times and in some circumstances, the College may install CCTV surveillance. . This will be in order to safeguard the health, safety and security of employees, students, other members of the public or College premises, equipment, systems or finances.

The Director of IT & Estates will ensure that all legal obligations are met when using CCTV. This includes acting in accordance with Data Protection Legislation, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. The College will also ensure that it does not act in a way, without reasonable and proper cause, which is likely to damage the relationship of mutual trust and confidence with employees.

Prior to the installation of CCTV on College property, Director IT & Estates must complete a Data Protection Impact Assessment. This should identify the following:

- The purpose for the monitoring and the likely benefits
- Likely adverse impacts
- Alternative ways in which the purpose might be achieved
- The obligations which will arise from monitoring
- A judgement on whether the decision is justifiable.
- Reference to clear procedures for strict confidentiality and security obligations of those individuals involved in the monitoring.
- The arrangements for processing and storage of the data.
- The arrangements for informing individuals that the monitoring is in place.

Covert monitoring (where the individual is not aware that the monitoring is taking place) will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity. If such monitoring is envisaged, this must be authorised by the Executive or Governing Body; carried out for a specific timeframe as part of a specific investigation and involve only a minimum number of people. In addition, the risks of intrusion on other individuals must be considered.

If this form of monitoring inadvertently brings up evidence of other malpractice, this evidence should not be used unless it is a case of gross misconduct. Where the misconduct is minor in nature, the use of this type of footage to discipline individuals will not be allowed.

5.6 Quality and retention of personal data

The College, via Asset Owners, will use reasonable endeavours to ensure that personal data is kept up to date and accurate, having regard for student and staff responsibilities for informing the College of changes to personal data, and regard to the purposes for which the data is processed.

College staff should also have regard for the College's Archiving & Retention Policy, with Asset Owners contributing to policy review to ensure that personal data is only retained for as long as necessary.

The Head of Business Intelligence will ensure that appropriate measures are in place to restrict access to management information reports as necessary, assessing the appropriate methods and implementing accordingly. Reported sensitive personal data content will be anonymised, with access to identifying information being restricted via a formal authorisation process.

5.7 Privacy Notices

The College will implement a layered approach to publishing privacy notices. This means that the College will publish main privacy notices on the College website – with sections relating to student applications, staff applications, students and employers. Where further information is collected, a shorter privacy notice will be visible to the data subject either via a 'pop up' or similar on the website; a clearly visible notice on a collection form or a verbal message which follows an agreed script.

Main privacy notices will include the College's details (as data controller), the contact details of the College's Data Protection Officer, the purposes of data processing (how data is used), links to the College's data retention policy, how it is stored, the legal bases for data processing, categories or what categories of people will receive or have access to the data and individual's rights.

Where the College processes data that is not directly obtained from the data subject, the College will include the source of the personal data and details of any profiling or automated decision making.

Privacy notices can be communicated verbally, in writing, through signage or electronically. The College will use clear and plain language in all cases.

Records will be maintained by Head of Data Management, which detail the content of the main privacy notices displayed on the College's website and the applicable dates. Asset Owners are responsible for assessing the requirement for a supplementary privacy notice, progressing implementation in line with the College's data protection principles. Where a privacy notice is communicated verbally, this will be in line with an agreed script and the Asset Owner is responsible for keeping a record of that script and the applicable dates, should it be amended, removed or replaced. Asset Owners must put procedures in place to ensure that verbal privacy notices are being communicated.

6. Technical and Organisation Measures

Data Protection Legislation identifies the principle of integrity and confidentiality. This means that personal data should be processed in a manner that ensures appropriate protection against unauthorised or accidental loss, inappropriate destruction or damage, using appropriate technical and organisational measures.

6.1 Physical and Environmental Security Measures.

Personal data processed by the College shall be subject to physical and environmental security measures. This relates to ensuring the physical and environmental security of physical data records and IT equipment, which may give access to personal data. Measures include, but are not limited to the following:

- Identification and necessary physical security to establish "Secure Areas" as required
- Procedures to ensure the security of College IT equipment – purchase, delivery, issue, use, maintenance, disposal or re-use.
- Procedures to ensure network cable security
- Procedures to ensure the security of College IT equipment off-site

- Procedures to be followed when using personally owned devices (BYOD) and when working off-site.
- Provision of lockable furniture or suitable alternative for physical personal data records, as appropriate.

6.2 Data Sharing

A Data Sharing Agreement should be in place that details the circumstances and arrangements for the College to share personal data with other organisations or persons where this is not covered by a contractual agreement. Often this is in line with the College's public task or obligations. In all such circumstances, the processing should be recorded on the Personal Data Register and the agreed College form should be completed and recorded before sharing takes place. The Asset Owner in the relevant work area is responsible for ensuring a risk assessment of activities under these circumstances.

Where the College receives personal data from a third party, the College will cooperate by providing detail of data protection measures to be applied. This may be recorded in a data sharing agreement or equivalent issued by the third party. The Asset Owner of the relevant work area is responsible for ensuring the necessity of the data received in line with the purpose of processing.

6.3 Data in transit

All staff must have regard for the security and safety of personal, sensitive personal or confidential business critical data when transferring to or from a third party. It must be protected during transfer across all types of communication methods.

6.3.1 Electronic data transfer or sharing with third parties

Personal and confidential information must be protected from interception, copying, modification, misrouting and destruction during any transfer. This could be achieved by:

- encryption of the information itself,
- using encrypted transport facilities or secure file exchange / portal methods or,
- a combination of these methods.

When encryption of the data is required, this should be achieved using recognised and accredited encryption software. At the point the file is encrypted to such a standard, it may be sent across an open network – e.g. email, FTP or OneDrive. Any required file password must be sent via a different medium, e.g. SMS, over the phone, email if the file is in O365 and shared, or sent in a different email.

Where such electronic data transfer or sharing with external parties is required, the Asset Owner should liaise with IT Support staff to ensure the appropriate encryption and/or mechanism for transfer via a secure portal.

All College provided file transfer mechanisms will run malware-detection programs:

- On servers and systems provided for file transfer

- Desktop devices, including Laptops and netbooks

6.3.2 Data transfer with third parties using other media

Post or courier services: any media containing personal, sensitive personal and/or confidential data that is transferred via postal systems or couriers must be sent by recorded delivery. If the data is stored on portable media, it must be encrypted.

Phone messages containing personal, sensitive personal or confidential information must not be left or recorded. This would constitute an unacceptable risk to the security and safety of that information, as it may be accessed by unauthorized persons, stored on communal systems, or stored incorrectly as a result of misdialling.

Fax machines should not be used for transmitting any confidential, personal or sensitive personal data, unless explicitly and contractually required to do so, in which case authorisation must be obtained from the Head of Data Management.

6.4 IT Security

6.4.1 Network Security and Vulnerability Assessment

The College network is connected to the internet via JANET (Joint Academic Network).This connectivity is managed and controlled by the JANET computer Security and Incident Response Team (SIRT). The College will fully cooperate, assist and seek advice from SIRT to ensure effective monitoring of connections, and the management of any suspicious activity or threats.

The Director of IT and Estates ensures:

- Appropriate and secure access to the College's network.
- An appropriate firewall between internal and external connectivity that protects the College's network from network penetration, malware and viruses.
- Network monitoring which raises alerts of systems failures or anomalies
- Software which monitors the connection of rogue devices
- A monitored, College Wi-Fi network with secure hardware and secure authentication
- Separation of network traffic as appropriate to maximise security

6.4.2 Malware Prevention

The Director of IT & Estates will ensure the use of appropriate technologies and products to ensure that the College network and data is protected from damage caused by 'malware' including viruses. Automatic virus and malware protection will be maintained, and measures put in place to ensure the security of any received files or removable storage.

All software and firmware updates should be applied promptly as provided by manufacturers and vendors.

6.4.3 Removable Media Controls

A secure College portal (GC Portal) is provided which enables staff to access any necessary personal data in a secure environment without the need to use removable media. By exception, where personal data must be stored on removable media, either for 'transit' purposes (para 6.3) or another exceptional circumstance, encrypted media formats must be used. The Asset Owner must authorise this use of removable media and liaise with the IT Support Team in order to implement an appropriately secure solution. Personal data stored on College servers must not be downloaded onto personally owned storage.

Removable media such as USB sticks, memory cards or portable drives are used in the College primarily for storing large files where latency of transmission could cause issues. Use of such media is restricted to resources and non-personal data such as student work, although it is recognised that such work may be attributable to a named student.

6.4.4 Secure Configuration

College systems must be controlled using secure industry standard operating systems for network configuration, user access and directory permissions. Security patches for these systems must be applied without delay when provided by suppliers as practicably appropriate, using industry standard automated deployment tools. All updates and changes to College systems should be tracked using change control. In additional all servers and clients should be tested before updates are released.

All College network users must sign the College's Communications and Acceptable Use Policy. This identifies the user's responsibilities for:

- The security of their issued username and chosen password
- Ensuring that College network usernames and passwords are not stored or set to be remembered when using generic accounts

6.4.5 Managing User Privileges and Access Controls

In line with the College's data protection principles, all user privileges and access must be controlled to protect College data and systems. Measures include, but are not limited to the following:

- Industry standard operating systems used to apply unique user permission and security group membership permissions.
- Measures to ensure safeguards when creating new user accounts.
- Measures to maintain user password security.
- Procedures to ensure that network access is removed when users cease to be employees of the College, or access is changed in line with changed circumstances.
- A clear authorisation process that obtains the appropriate written permission to give, or extend, access to file content.

- High-level privileges restricted as deemed necessary by the Director of IT & Estates.

6.4.6 Incident Management

A data breach must be reported using the College's Data Breach procedure (see para seven below). During the assessment of the threat, the DPO will liaise with IT staff, acting appropriately to contain any threat to the College network or files.

The Business Recovery Plan must be followed as necessary to communicate and manage any incident and restore College operations. This Plan is tested and audited on a regular basis as determined by the Executive.

6.4.7 Off-Site and Mobile Working

The College provides a facility for staff to access the College network from non-site locations via a secure portal, using a virtual staff desktop (GC Portal). Personal data can be accessed and processed via this secure portal as necessary as part of working procedures.

6.4.8 Monitoring IT Security

Director of IT & Estates will ensure the appropriate monitoring and reporting of incidents, breaches or issues that increase or constitute risks to the College network, systems or data integrity. Network activity will be monitored with firewall ports and configuration adjusted accordingly. Access groups should be regularly reviewed, and login activity monitored. Reporting will also be available which monitors timely software and firmware updates.

6.5 Data Protection by design and Data Protection Impact Assessments (DPIAs)

The risks to personal data safety and security should be assessed at the early stages of any project or initiative. This consideration of privacy implications at the design phase of any new system, policy or project, enables the early identification of potential problems and consideration of simpler and less costly measures to address risks. This proactive approach aims at:

- Preventing privacy risks occurring.
- Ensuring that personal data is protected as part of a process driven framework where privacy is the default.
- Considering privacy and embedding in the design phase of any initiative.
- Protecting personal data during the full 'life-cycle' - from collection through to retention and erasure.
- Providing transparency and visibility of processing

Where the project or initiative involves data processing that is likely to result in a high risk to the rights and freedoms of individuals, a DPIA must be completed. Where the risk assessment carried out by the Asset Owner indicates a 'medium' risk, it is good practice to also complete a DPIA in these circumstances.

The Asset Owner or Project Director is responsible for ensuring that the DPIA is carried out, and must seek advice from the DPO. This advice should be recorded. The DPO will monitor, audit and record DPIAs, reporting to the Executive should

there be any impending risk to demonstrating compliance with Data Protection Legislation.

6.6 Procurement

A written contract will be in place where a data processor carries out any processing of personal data on behalf of the College as Data Controller. The contract will include as a minimum the clauses as required within Data Protection Legislation:

- Documented instructions on use of data
- Security measures in place
- Controller authorises use of sub-contractor
- Deletion or return of data after end of the contract.
- Make available to the College all information necessary to demonstrate compliance and allow for and contribute to audits conducted by the College or another auditor mandated by the College.
- Assist the College in carrying out its obligations with regard to requests by data subjects to exercise their rights under chapter III of the GDPR; and in carrying out Data Protection Impact Assessments.
- Notify the College without undue delay after becoming aware of a personal data breach.

The College will only enter into agreements with data processors that provide sufficient guarantees to implement the appropriate technical and organisational measures in order to meet the requirements of Data Protection Legislation and protect the rights of the data subject(s).

The Financial Controller will carry out checks to ensure compliance.

Where the College contracts with self-employed individuals, they will be required to operate in line with all the College's policies as they relate to data protection.

6.7 Training and Awareness

This Data Protection and IT Security Policy, and other related College policies (including the College's Communication and Acceptable Use Policy), will be covered during the induction of all new staff. All staff must have regard for the Data Protection and Information Security Policy and must undertake mandated training as determined by the Director of HR.

In addition, managers identified as Asset Owners will be briefed by the College's DPO on their responsibilities and kept updated with any changes to data protection or IT security policies, procedures or principles.

The College's DPO will be given opportunities and access to continuous training in order to stay up to date with developments within data protection and privacy.

From time to time, the DPO through the Executive team will arrange and promote campaigns to engage staff and students, raising their awareness of the importance of security and establishing a privacy-conscious culture.

7. Data Breaches

A personal data breach is defined as a breach of security leading to the inappropriate destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The College's data protection principles and procedures aim to minimise the possibilities of a data breach. However, the College will ensure that all staff are aware of what constitutes a person data breach, and their responsibilities to report any such incidents. This includes temporary, or agency staff, volunteers or contractors working for, or on behalf of the College. Members of staff who process personal or sensitive personal data for the purposes of College business must take appropriate steps to ensure that no unauthorised or unlawful processing, accidental loss, destruction of, or damage to personal data occurs. A Data Breach Procedure must be in place and should form part of mandated training.

All staff should be aware that disciplinary proceedings may result following investigation of a data breach, in line with the College's Disciplinary Policy.

8. Individual Rights

8.1 Subject Access Rights

Staff, students and other individuals have the right under Data Protection Legislation to access any personal data that is processed by the College, in either an electronic or a paper format. A person who wishes to exercise this right must contact the College's Data Protection Officer in writing; a Subject Access Request (SAR) form is available for this purpose. The College, via the DPO, will comply with requests for access to personal data as quickly as possible and without undue delay, but will ensure that a response is provided within one month of receipt of the request. That period may be extended by two further months where necessary. Information will be provided free of charge. Where a request is manifestly unfounded or excessive, the College may charge a reasonable fee taking into account the costs of providing the information, or may refuse to act on the request.

All Subject Access Requests must be managed, or directed by the College's Data Protection Officer, but all College staff should have regard for the College's "Procedure relating to personal data requests from individuals".

8.2 Other Individual Rights

Under Data Protection Legislation, an individual has specific rights relating to the personal data concerning him or her that is processed by the College. Under some circumstances, the College may apply some restrictions to these, and the advice of the College's Data Protection Officer should always be sought to ensure full compliance with relevant legislation.

Individual rights include:

- **Right to rectification –** right to rectification of inaccurate personal data processed by the College, concerning him or her
- **Right to erasure** – the right, in some circumstances to require the College to erase personal data concerning him or her.
- **Right to data portability –** the right , in some circumstances, to have personal data concerning him or her transmitted to another data controller
- **Right to object –** the right to object, in some circumstances, to the processing of personal data concerning him or her, on grounds relating to his or her situation

- **Rights relating to automated decision-**making and profiling – the right not to be subject to a decision based solely on automated processing, including profiling, in certain situations.

9. Review and Monitoring Data Protection in the College

A review and monitoring cycle should be clearly defined which outlines the key controls and reporting giving assurance to the Executive Team and the Governing Body that data protection risks are being managed effectively within the College. Controls should be specified at three levels: Operational, Strategic, Independent & Objective.

10. Related Policies and Procedures

This policy should be read in conjunction with the following College documents that can be found on the College's SharePoint 'Policies' site,

- Communication and Acceptable Use Policy
- Access to Information and Publication Scheme
- Disciplinary Policy
- Code of Conduct
- Archiving and Retention Policy
- Social Media Policy
- Student Agreement and Code of Conduct

The Head of Data Management will maintain a suite of procedures that support the practical application of the College's Data Protection and IT Security Policy.
These will include but are not limited to the following:

- Physical & Environment Security Measures,
- Data Sharing Procedure,
- Data Protection Impact Assessment Procedure,
- Data Breach Procedure,
- Procedures relating to personal data requests

Appendix A

Data Protection Legislation throughout this document means

1. Unless and until the General Data Protection Regulation((EU)2016/679 (GDPR) is no longer directly applicable in the UK, the GDPR and nay national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK; and then
2. Any successor legislation to the GDPR or the Data Protection Act 1998.

Glossary: Data Protection Terms

Anonymous Data
Sets of data that are amended in such a way that no individuals can be identified from those data (whether directly or indirectly) by any means or any person. Data where no individuals can be identified are outside the scope of GDPR.

Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Controller
The natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Concerning Health
Personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status. This expressly covers both physical and mental health.

Data Processor
Any natural or legal person (other than an employee of the data controller), public authority, agency or any other body processes personal data on behalf of the Data Controller.

Data Subject
An individual who is the subject of the personal data

Personal Data
Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Online identifiers including IP addresses, cookies etc. are regarded as personal data if they can be (or are capable of being) linked back to the data subject. There is no distinction between person data about individuals in their private, public or work roles.

Processing
Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data

b) retrieval, consultation or use of the information or data
c) disclosure of the information or data by transmission, dissemination or otherwise making available or
d) Alignment, combination, blocking, erasure or destruction of the information or data.

Profiling
Any automated processing of personal data to determine certain criteria about a person. In particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation
The method by which personal data is processed such that it can no longer be tied to an individual data subject without linking to additional data. This is still treated as personal data because this enables identification of the person albeit via a key. If the 'key' that enables re-identification of individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be low, and so the levels of protection required for those data are likely to be lower.

Sensitive Personal Data or Special Category Data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences or convictions are not in the GDPR 'special categories' but are subject to similar restrictions.