Data Protection Policy
June 2023

1. Introduction

1.1. Carmel College needs to collect and use certain types of information about people with whom it deals. These include current, past and prospective students and parents, staff, suppliers, and others who use the facilities and with whom it communicates. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, unintended modification or disclosure.

1.2. The information collected is used to allow the College to monitor performance, achievements, health and safety and other statutory requirements. It also needs to process information so that staff can be recruited and paid, lessons organised and legal obligations to funding bodies and the government complied with.

1.3. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This Policy sets out the obligations of Carmel College regarding data protection and the rights of staff, students and other workers in respect of their personal data under the **General Data Protection Regulation ("the Regulation")** from 25th May 2018.

2. Status of the policy

2.1. Carmel College and all staff, students, or others who process or use any personal information, must ensure that they follow these principles at all times. All references to staff include all current, past, and prospective staff, full time and part time staff as well as agency staff, trainees and contractors. All references to students include all current, past and prospective students, whether full-time or part-time.

2.2. This policy does not form part of the formal contract of employment, but is a condition of employment that employees will abide by the rules and policies made by the College. Employees may be subject to disciplinary procedures if found to be in breach of it.

2.3. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter initially with the person nominated to protect that data, and then with the designated Data Protection Officer. If the matter is not resolved it should be raised as a formal grievance.

2.4. Agreement to Carmel College processing some specified classes of personal data is a condition of employment for staff and is a condition of acceptance of a student onto a programme of study. Both staff and students sign to this effect on entry to employment and programme respectively. Employment, or course places, might be withdrawn if an individual refuses consent without good reason as data processing is undertaken for the performance of the contract with the Data Subject. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

2.5. Carmel College can only process personal data with the consent of the individual. In particular if the data is sensitive (e.g. information about a person's health, racial or ethnic origin, or their criminal convictions) express consent must be obtained before processing. This information is needed to ensure that the College is a safe place for everyone, and to allow the operation

of other College policies such as the Equality and Diversity policy. Carmel College has a duty of care to all staff and students.

2.6. The storage and processing of information relating to safeguarding issues is discussed in the College's Safeguarding and Child Protection Policy. Child protection records are normally exempt from the disclosure provisions of GDPR. Examples of information which it may be appropriate to withhold include information that would reveal that the child is at risk of abuse where disclosure of that information would not be in the child's best interest, or where the information might cause serious harm to the physical or mental health of the student or another individual. The College also reserves the right to disclose sensitive information about an employee or a student regarding their health if there is a serious risk of harm to them or others that over-ride the duty of confidentiality, and if the circumstances make it impractical to seek explicit consent. The College also reserves the right to share information, both internally and externally, about vulnerable individuals who may be identified as at risk due to our Prevent duty.

3. The College as Data Controller

3.1. Carmel College is the data controller under the Regulations, and the Governing Body is therefore ultimately responsible for its implementation.

3.2. The types of information held by the College and how they are used are detailed in the College's registration issued by the Information Commissioner (ICO) under the reference Z6391538. The registration papers are available via the Information Commissioner's Office (ICO) website (www.ico.org.uk) or from the designated Data protection Officer.

3.3. The designated Data Protection Officer will deal with the implementation of agreed policy and day-to-day matters along with the nominated staff:

Designated Data Protection Officer	Vice Principal (Finance, Systems and Resources)
Deputy Designated Data Protection Officer	College HR Manager

3.4. Key nominated data protection staff:

Staff records	College HR Manager
Student records	College MIS Manager
Student welfare records	Designated Safeguarding Lead
College examination records	College Examination Manager
College IT data/infrastructure	College IT Manager
College marketing materials	College Marketing, Liaison & Admissions Manager
College financial records	College Finance Manager
College health and safety records	College Estates Manager

3.5. The College maintains data in secure conditions and processes and discloses data only within the terms of its notification to the Information Commissioner.

3.6. The College will keep written internal records of all personal data collection, holding, and processing, which will incorporate the following information:

- The purposes for which the College processes personal data
- Details of the categories of personal data collected, held, and processed by the College; and the categories of data subject to which that personal data relates
- Details of the data storage locations of personal data.
- Details (and categories) of any third parties that will receive personal data from the College
- Details of any transfers of personal data to outside of the United Kingdom including all mechanisms and security safeguards
- Details of how long personal data will be retained by the College
- Detailed descriptions of all technical and organisational measures taken by the College to ensure the security of personal data

The designated Data Protection Officer keeps the lists of the types of records and the person responsible for its security.

4. Principles of data protection

The College is committed to the principles of data protection, as stated in the Regulation:

4.1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject

The Regulation states that processing of personal data by the College will be lawful if at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary to protect the vital interests of the data subject or of another natural person
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes

- The College collects and processes the personal data set out in the appendices of this Policy. This may include personal data received directly from data subjects (for example,

contact details used when an applicant communicates with us) and data received from third parties (for example, references).

- The College only processes personal data for specific purposes, or for other purposes expressly permitted by the Regulation. The purposes for which the College processes personal data will be outlined to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

- The College will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects

4.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay

- The College will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

4.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject

- The College will not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

4.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

- The College will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5. Rights of Individuals - data subjects

The Regulation sets out the following rights applicable to individuals:

5.1. The right to be informed

- The College will ensure that the following information is provided to every individual (data subject) when personal data is collected. Where the personal data is obtained

from the individual directly, the information will be provided at the time of collection. Where the personal data is not obtained from the individual directly (i.e. from another party), the information will be provided at the time of the first communication, or not more than one month after the time at which the College obtains the personal data.

- Details of the College including, but not limited to, the identity of the College's Data Protection Officer
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in the Appendices to this Policy) and the basis justifying that collection and processing
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed
- Where the personal data is to be transferred to one or more third parties, details of those parties
- Where the personal data is to be transferred to a third party that is located outside of the United Kingdom, details of that transfer, including but not limited to the safeguards in place
- Details of the length of time the personal data will be held by the College (or, where there is no predetermined period, details of how that length of time will be determined)
- Details of the individual's rights under the Regulation
- Details of the individual's right to withdraw their consent to the College's processing of their personal data at any time
- Details of the individual's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation)
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences. The College does not utilise automated decision making processes.

5.2. The right of access

Individuals have the right to access any personal data that is being kept about them either on computer or in manual filing systems. They are entitled to a description of the information, what it is used for, who it might be passed to, and any information about the source of the information, so that the data subject can verify the lawfulness of the processing. A request in writing for a copy of any such information is called a data **Subject Access Request**.

- Any individual who wishes to exercise this right should use the form included in Appendix 1 of this policy. All subject access requests received must be forwarded to the Data Protection Officer, and the identity of the person making the request verified, using "reasonable means".
- The College will supply a copy of the information requested free of charge without delay and at the latest within one month of receipt. The period may be extended by a further two months where requests are complex or numerous, but the data subject will be informed within one month of the receipt of the request with an explanation of why the extension is necessary.
- Where SARs are manifestly unfounded or excessive, in particular because they are repetitive, the College will either charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond. If the College refuses to respond to a request, an explanation will be provided to the individual,

informing them of their right to complain to the supervisory authority without undue delay and at the latest within one month.

- Individuals have the right to request to see emails which concern or mention them that had not originally been sent directly to them, copied to them, or were received by them. The return would include any emails in a person's "delete" box, but not those deleted from the system. As such emails should not be considered confidential.
- Emails retrieved as a result of a request will generally be redacted according to the following principles:
  - no staff names are included on the printed copies that are not current employees of the College;
  - no student names are included on the printed copies;
  - that it is reasonable to present the information, and not unfair to disclose it based on the expectations of the individual sender and receiver at the time of sending. If doubt exists over this then consent to transmit will be sought.

5.3. The right to rectification

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. The College will respond to a request for rectification within one month, though as above this can be extended by two months where the request is complex.
- If the College has disclosed the personal data to others, the College will contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

5.4. The right to erasure (the 'right to be forgotten')

- An individual has the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Unless there are grounds to refuse erasure, the College will respond to a request for erasure within one month of receipt, though as above this can be extended by two months where the request is complex. If the College has disclosed the personal data to others, the College will contact each recipient and inform them of the erasure - unless this proves impossible or involves disproportionate effort.
- Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which the College originally collected/processed e.g. were a student application is not followed through
- When the individual withdraws consent to the College holding and processing the data
- When the individual objects to the College processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order for the College to comply with a particular legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

5.5. The right to restrict processing

- Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the College will continue to store the personal data, but not further process it, retaining just enough information about the individual to ensure that the restriction is respected in future. If the College has disclosed the personal data to others, the College will contact each recipient and inform them of the restriction - unless this proves impossible or involves disproportionate effort.

5.6. The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data, which they have provided to the College, for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. If the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.
- Unless there are grounds to refuse erasure, the College will respond to an individual's request for their data within one month of receipt, though as above this can be extended by two months where the request is complex. The College will provide the personal data in a structured, commonly used machine-readable form e.g. CSV, or PDF formats. Machine-readable will enable software to extract specific elements of the data, which will enable other organisations to use the data.
- The College will provide the information free of charge. If the individual requests it, the College may transmit the data directly to another organisation if this is technically feasible.

5.7. The right to object

- Individuals have the right to object on "grounds relating to their particular situation" to the College processing their personal data based on legitimate interests (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- The College will stop processing the personal data unless there is compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claim. The College will stop processing personal data for direct marketing purposes as soon as it receives an objection. The College does not need to comply with an objection to the processing if it is conducting research where the processing of personal data is necessary for the performance of a public interest task.

5.8. Rights with respect to automated decision-making and profiling.

- GDPR applies to all automated individual decision-making (making a decision solely by automated means without any human involvement), and profiling (automated processing of personal data to evaluate certain things about an individual). The College does not currently employ automated decision-making systems nor employ profiling systems.

6. Retention of College data

6.1. College will keep some forms of information for longer than others, for example, based on statutory requirements, professional guidance and best practice principles. "Necessity" will inform data retention periods and will be decided in the light of requests to access the data and reviewed in the light of best practice employed across the sector. For the majority of its information about students, the College is guided towards a data storage period of six years from the date of last entry, or if appropriate date of student birth + 25 years. The data is held within the MIS system. The processing of student data is currently under review as a new student management system is implemented. HR practice will inform the retention of staff records. HR data from 2009 is held within CINTRA IQ, with older data archived. Data retained will be regularly reviewed so that information that is no longer authorised to be retained under the policy is securely destroyed or transferred to secure archives. A senior leader will approve the removal and subsequent destruction or archiving. This action will be documented.

6.2. Details regarding the College's eventual retention periods for classes of document and personal information are provided in the Appendix. The Data Protection Officer will oversee the person designated to be in charge of specific data classes and review with them the retention period for the data.

6.3. In some instances, Carmel College will make the decision to keep some central records indefinitely. This will be reviewed in line with the policy guidelines and shown in Appendices 5 and 6.

7. Keeping data secure

7.1. All staff, students, or others who process or use any personal information for the College, will be made fully aware of their responsibilities under GDPR. They will have access to a copy of this policy and will be trained to handle the data appropriately. They will have appropriate supervision.

7.2. The College's methods of collecting, holding and processing personal data will be regularly evaluated and reviewed. Following the 2022 cyber-attack the following actions were taken with respect to data security:

- Implementation of Sophos Managed Threat Response (MTR) for remote 24/7 monitoring of college infrastructure, including workstations, servers and laptops,
- Purchase of Zero Trust Network Access (ZTNA) to allow secure remote connections for staff and possibly students remote access,
- Purchase and implementation of new Backup Infrastructure including Veeam Backup and Recover, Synology Short-Term on-site storage unit and Synology Long-Term on-site storage unit, implementation of Blocky to limit access to backup repositories
- Backups are taken at the following instances daily, held on-site at two locations which are independently secured. A cloud-based and an off-site backup is being investigated.
- College systems will be migrated to cloud-based provision, where possible and effective. The following systems are already cloud based: CintraIQ (Payroll), 3CX (Telephony), College website, Symmetry Bluecube (Finance).

7.3. All staff and students will have their own individual log-in and password for access to the network. Staff and student responsibilities with regard to their network accounts are outlined, and compliance is agreed to, via the College's **IT and Social Media Acceptable Usage Policy**. Under no circumstances should any passwords be written down or shared between

any employees, agents, contractors, or other parties working on behalf of the College, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

7.4. The computerised CCTV recordings are considered as personal data under the Regulation. Recordings on the CCTV files will only be used as outlined in the College's **Code of Practice: CCTV equipment.** Copies of recordings and prints can be retained for up to 6 years where criminal proceedings are possible. Otherwise, recordings are permanently erased on a rolling basis within 30 days.

7.5. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using software provided by the College.

7.6. To facilitate secure remote working the college will follow the recommendations supplied by the Information Commissioner's Office. Namely: clear policies, procedures and guidance for staff; up-to-date versions of remote access solution; unique and complex staff passwords; multi-factor authentication configured as appropriate. Our cloud storage solution: will not be set to public, accessible only after authentication; only key staff will have full access to the storage area; we will not use any default root or administrative accounts for day-to-day activities. Our remote desktop: will have account lockouts in place; will not have generic usernames for privileged accounts, disabling any built in or default administrator accounts; allow access only to staff who require it. Our remote applications: will not allow access to Windows administrative tools; will not use shortcut tool to open non-authorised applications; not have usernames and passwords in files or folders. Remote working will operate via Zero Trust Network Access (ZTNA) to allow secure remote connections. For our email solution: we will review and implement NCSC and JISC guidance on defending against phishing attacks; consider our rules relating to email forwarding; advise staff to use the college account, not their own email or messaging accounts. The college has achieved Cyber Essentials certification.

7.7. Data which has not been modified for a long time, and no longer has an identifiable use, will be deleted according to an IT procedure: from July 2023 an automated delete process will remove any files that have not been modified (saved) in the last 8 years. These deleted files will still be available within backup storage for a further two years, but only accessible via IT services. After ten years from last saving they will be fully removed.

7.8. Responsibilities of staff

7.8.1. The College cannot be held responsible for any errors in the personal data held unless the member of staff has informed the College about them. Staff are responsible for:

- checking that any information that they provide to Carmel College in connection with their employment is accurate and up to date;
- informing Carmel College of any changes to the information which they have previously provided, e.g. changes of address;
- checking the information that the College may send out from time to time giving details of information kept and processed about staff.

7.8.2. Undertake training as directed by college e.g. annual Smartlog training.

7.8.3. If, and when, as part of their responsibilities staff collect any information they must comply with the data protection principles and any associated guidelines. Staff must ensure that any personal data which they hold is kept securely; is needed; is adequate but not excessive; and that personal information is not disclosed either orally or in writing to any unauthorised third party. Information should only be retained when necessary and disposed of appropriately when no longer needed. Examples of information collected by teaching departments / staff are:

- students work;
- opinions about the ability of students e.g. reviews; interim reports;
- references from external bodies;
- details about personal circumstances e.g. written notes.

7.8.4. Subject Tutors and Heads of Department must take specific care to ensure that permission has been obtained from the students for the use of any material or information for marketing purpose by a teaching area and that the information is appropriate.

7.8.5. When work external to College is being undertaken by students, or when any external agencies come within Carmel College to work with students, staff must ensure that the information supplied is appropriate and that it will be kept secure by the external agency. The students must be aware that the information is being supplied e.g. student work placements.

7.8.6. With regard to the publication of examination results, students are entitled to information about their marks for both coursework and examinations. Examination pass lists and grade classifications must be published only in aggregated form unless the individual has consented. Examination results may not be divulged on the telephone unless there is prior agreement to do so. The results may only be divulged, by the Exam Office / Head of Department / or Subject Tutor, to the student to whom they relate or to another authorised person providing security measures to confirm their identity have been fulfilled.

7.8.7. When using the internet and Web based services and in particular those that require the transfer of personal data outside of College, staff should exercise caution and permission to transfer such data should be sought from the Data Protection Officer. As a general rule, if such sites are to be used then the student should be solely responsible for choosing the site and entering their own data, rather than the College.

7.8.8. Staff should not share logins to the network and special care must be taken when accessing the Civica REMS system or the CEDAR / Connect student management systems. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it. Teachers should pay particular care in class and freeze the data projector ~~screen~~ if accessing email, Civica or other non-teaching files such as student notes.

7.8.9. Care must be taken by all staff involved in performance management reviews to ensure that the information is kept confidential and secure via the CINTRA system. CINTRA should only be accessed in staff offices and the screen should not be left unattended.

7.8.10. All staff are responsible for ensuring that any sensitive or personal data which they hold, or for which they are responsible, is kept secure. At College:

- if it is not possible to computerise, sensitive information should be kept in a locked filing cabinet or drawer e.g. specific information from external agencies
- if it is computerised it should be password protected and the password kept secure e.g. our network is password protected and an appropriate password policy operated
- if computerised, then the computer itself must be kept in suitably secure conditions e.g. data must not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided; personal information must not be transferred to the local drives of home computers
- care must be taken when data is transferred through the College network to ensure that discrepancies are not allowed to arise
- if information is to be gathered through, or used on a website, then appropriate measures must be in place to control access and prevent unauthorised disclosure.

7.8.11. When sensitive or personal data is required at any location outside of College staff must:

- use the secure remote access to the management information system or the learning platform e.g. a tutor should write reviews directly onto the review section of CONNECT or CEDAR.
- if secure remote access is not possible, users must only remove or copy personal data from the College if permission has been sought from the Data Protection Officer and the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location e.g. IT Services have encrypted memory sticks. Personal data must not be permanently stored on any mobile device.
- keep laptop computers turned-off and secure when not in use to prevent opportunistic theft
- keep home computers secure at all times to ensure that unauthorised persons cannot view the data
- keep personal computer(s) secure using up-to-date operating systems, web browsers, and security software - anti-virus and anti-spyware. e.g. IT services will provide advice;

7.8.12. When remote working from college staff should note the following Information Commissioner's Office top tips:

- Follow Carmel's policies and guidance relating to Data Protection and the Acceptable Use of IT.
- Only use approved technology, hardware and software. Ask IT services if in any doubt about suitability.
- Consider confidentiality when holding conversations or using a screen, ie. can you be overheard or can the screen be seen by others?
- Take care with any print outs, make sure they are disposed of safely.
- Do not mix your work data with your own personal data.

- Do not store any sensitive data at home, use the college preferred access/storage solutions e.g remote access. If absolutely necessary, then seek approval and keep information under lock.
- Be extra vigilant about opening web links and attachments in emails and other messages e.g. beware of phishing.
- Follow our password protocols.
- Use the communication facilities provided by Carmel if possible. Ensure that any system used is secure when sharing data. IT services will support you in this.

7.8.13. Unauthorised disclosure of personal data is a breach of the Data Protection Act and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

7.9. Responsibilities of students

7.9.1. Students are responsible for:

- checking via their ILP portal that any information that they provide to Carmel College in connection with their studies is accurate and up to date.
- informing Carmel College of any changes to the information which they have previously provided e.g. changes of address;
- checking the information that the College may send out from time to time giving details of information kept and processed.

7.9.2. The College cannot be held responsible for any errors in student personal data unless student has informed the College about them and they have not been rectified.

7.9.3. If a student gathers another person's data as part of a College assignment, then the information obtained must be appropriate, kept secure, and the person whose data it is must be aware that the information is being used and how it is to be processed. Information should only be retained when necessary and disposed of appropriately when no longer needed.

7.10. Responsibilities of agents, contractors, or other parties

7.10.1. All agents, contractors, or other parties working on behalf of the College handling personal data must ensure that any, and all, of their employees who are involved in the processing of personal data are made fully aware of their individual responsibilities, and are held to the same conditions as those relevant employees of the College arising out of this Policy and the Regulation

7.10.2. Where any agent, contractor or other party working on behalf of the College handling personal data fails in their obligations under this Policy that party will indemnify and hold harmless the College against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

7.10.3. Whenever the College uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities

and liabilities. The processor must not hire another processor to do the work, unless the controller has given permission to that act.

7.10.4. The College is liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. The use of a processor that states compliance with an approved code of conduct or certification scheme may help the College to satisfy this requirement.

7.10.5. Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

7.11. Transferring personal data

7.11.1. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

7.11.2. No personal data may be shared informally, and if an employee, agent, sub-contractor, or other party working on behalf of the College requires access to any personal data that they do not already have access to such access should be formally requested from the Data Protection Officer. Permission will only be given if they agreed to comply fully with the letter and spirit of this Policy and of the Regulation.

7.11.3. Special care must be taken when sending all emails containing sensitive personal data. These emails must be encrypted, and deleted when there is no longer a necessity for their storage. The email deleted items folder should also be "purged" after the file has been deleted to prevent recovery of the file.

7.11.4. Where sensitive personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery (signed for).

7.11.5. Generally, if personal data has to be transmitted to another location, firm, or country then seek advice from IT services.

7.12. Transferring personal data to countries outside the United Kingdom.

7.11.1. Now that the UK Brexit transition period has ended the Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.
On the 28th June 2021 the EU Commission decided that the UK's laws and systems for protecting personal data, as well as the legislation in place, designated the UK as 'adequate' to provide protection for personal data transferred from the EU under the EU GDPR. 'Adequacy' is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU. The adequacy decision will last to 27th June 2025.

7.11.2. The College may from time to time transfer personal data to countries outside of the European Economic Area. This transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country or territory that the European Commission has determined ensures 'adequacy' of level of protection for personal data.

- The transfer is to a country which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- The transfer is made with the informed consent of the relevant data subject(s)
- The transfer is necessary for the performance of a contract between the data subject and the College
- The transfer is necessary for important public interest reasons
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

7.13. Data protection impact assessment

7.13.1. Data protection impact assessments (DPIA) are a tool to help the College identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows the College to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. The use of DPIAs as an integral part of taking a privacy by design approach. A DPIA can address more than one project.

7.13.2. A data protection impact assessment form is included amongst the Appendices and contains:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the College.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

7.13.3. A data protection impact assessment must be carried out when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes (but is not limited to): systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals; large scale processing of special categories of data or personal data relation to criminal convictions or offences; processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals;

and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
- large scale, systematic monitoring of public areas (CCTV).

8. Data breach notification

8.1. The College needs to know as quickly as possible if a security incident has happened. Any problems should be reported immediately it is discovered to the nominated member of staff responsible for that data and hence to the Data Protection Officer.

8.2. If a significant data breach occurs that results in a risk to the rights and freedoms of the Data Subject(s), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

8.3. In the event that the data breach is likely to result in a high risk to the rights and freedoms of data subjects, (e.g., breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly, without undue delay, and following best advice.

8.4. In the event of a data breach, employees of College must not make any statements to the media regarding the incident. This includes postings on social media sites.

8.5. The following steps will take place when a data breach is noted:

8.5.1. CMT will review the incident to consider the risks.

8.5.2. a resolution team will be formed comprising staff with relevant experience who will address the technical, process and legal aspects of the issues at hand and devise and implement a plan of action. Support will be sought from external agencies were appropriate.

8.5.3. alongside this a communication plan will be formulated to ensure that all relevant members of staff in the organisation, associated parties including the college insurer and law enforcement agencies are informed to ensure a: rapid resolution; non-recurrence; limitation of damage; and protection of all users.

8.5.4. Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the College's Data Protection Officer (or other contact point where more information can be obtained)
- The likely consequences of the breach
- Details of the measures taken, or proposed to be taken, by the College to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

8.5.5. Following the incident, a debrief will take place, changes to any systems implemented and staff made aware of the changes.

9. Conclusion

9.1. This Policy sets out the obligations of Carmel College regarding data protection and the rights of staff, students and other workers in respect of their personal data under the General Data Protection Regulation ("the Regulation") and compliance with the Regulations is the responsibility of all members of Carmel College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Carmel College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

<table>
<tr><td>File Name/Path</td><td colspan="5">O:\Policies\Policies\2022-23 Policies</td></tr>
<tr><td>Intranet Path</td><td colspan="5">CONNECT > DEPARTMENT>COLLEGE POLICIES</td></tr>
<tr><td rowspan="2">Circulation List</td><td>Principalship</td><td>√</td><td>College Union Representatives</td><td colspan="2">√</td></tr>
<tr><td>Full Governing Body</td><td>√</td><td>HR Department</td><td colspan="2">√</td></tr>
<tr><td rowspan="2">Author/ Responsibility</td><td colspan="2" rowspan="2">Assistant Principal Curriculum</td><td>Date of Policy approval</td><td colspan="2">June 2023</td></tr>
<tr><td>Date next review due</td><td colspan="2">June 2024</td></tr>
</table>

Appendix 1: Data Protection – Subject Access Request Form

Date Request Received (Official use only)	
Date to be Processed by (Official use only)	

DATA PROTECTION - SUBJECT ACCESS REQUEST FORM

In order for us to process your request promptly please complete this form as fully as possible and return with the required proof of identification and fee to the address below.

Your details

Name .....

Address ……..…….....

Date of birth ……..

Telephone number ……..

Email ……..

Description of the information you require.

Please provide a description of the information you would like the College to provide you with, including what department(s) of the College you think hold this information e.g., HR/ MIS/ IT / academic department.

If you know, please specifically state the exact documentation reference to allow us to process your request promptly e.g., student/staff file in department.

……..

……..

……

……

……

……

……

Verification of Identity

As data controller, Carmel College has a legal obligation to protect any of your personal information it holds. To prevent any unauthorised disclosure, we are required to verify your identity. In order to allow us to do so please provide a copy of at least one of the following pieces of documentation. If you possess neither, please contact us ASAP (contact details below).

- Current passport

- Driver's licence

Please send this Subject Access request form to

Attention: Data Protection Officer
HR
Carmel College
Prescot Road
St. Helens
Merseyside
WA10 3AG

Email: hr@carmel.ac.uk

The information you provide on this form will be used to process your request. Summary information may be retained for statistical or audit purposes. By providing this information you consent to Carmel College storing your information for these purposes. Carmel College will process your data in accordance with the General Data Protection Regulation.

Appendix 2: Privacy Impact Assessment Form

What is the aim of the data collection/data sharing? What are the benefits to data subjects, the College etc?		
What data will be collected? How will this data be used?		
How will the data subjects' consent be obtained? Do existing Privacy Notices include this data collection/sharing?		
How will the data be collected?		
Where will the data be stored? (Both physical and electronic records)		
How and will the data be shared (Note both internal and potential external destinations). What security is in place to protect the data subjects' privacy?		
What process is/will be in place for the data to be amended?		
When and how will the data be deleted (Note Retention Period)		
What are the risks of collecting and processing this data (Individuals, Compliance, College etc.)		
What controls are in place to control the risks?		
Who is responsible for the collection, processing, reporting, amending and deleting this data?		
Signature:		Date:
Approved Yes/No	Data protection Officer signed:	Date:

Appendix 3: Data Breach Report Form

Date:	**Comments**
Outline of breach to include: When did the breach occur (date and time)? When was the breach discovered (date and time)? Who discovered the breach? How is it thought the breach occurred?	
Which data subjects are involved: (if multiple include a spreadsheet file/list etc) Indicate student/staff/parent etc.	
What data has been disclosed/lost?	
What action, if any, has been taken?	
Reported to Data Protection Officer by:	
Reported to Data Protection Officer date and time:	

Date and time received by DPO:	
Date and time to report to ICO if required:	
Does this breach result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage)?	Yes/No: If yes, notify the ICO
Date and time incident reported to the ICO:	
Does the data breach result in high risk to the data subjects?	Yes/No: If yes, notify the data subjects
What are the likely consequences of the data breach?	
Actions implemented to mitigate adverse impact of the breach to date:	
Actions to be implemented to mitigate adverse impact of the breach:	
Actions to prevent similar data breach occurring again:	
Signed	**Data Protection Officer**

Appendix 4: Overview of Data Collected

The College collects and uses data about its staff and students for the following purposes:

Staff

- Organisation and management of the College
- Payment of salaries and wages
- Medical history to ensure suitability for appointment
- CCTV monitoring of College campus
- Seeking improvements in health and safety
- Staff development
- Recording of equality and diversity information. This information is requested on a voluntary basis and is used to enable the College to evaluate the operation of its Equality and Diversity policy
- Recording of periods of sickness to enable payment of statutory sick pay
- Providing employment references
- Administration of pension schemes

Students

- College administration (includes personal and academic details) and management of academic processes (e.g. absence, reviews, examination entries and results)
- Provision of advice and support to students (e.g. careers guidance, bursary fund administration)
- Collection of fees (e.g. resit examination fees)
- Administration and provision of student identification cards
- CCTV monitoring of College site
- Recording of equality and diversity information. This information is requested on a voluntary basis and is used to enable College to evaluate the operation of its equal opportunities policy. This information is also requested by other relevant government bodies. To ensure that provision and support reflects the multi-cultural community
- Promotion of College courses
- Tracking of student progression, to establish the adequacy and relevance of courses in preparing students for post-College life. Provision of references for potential employers and UCAS application.

Disclosure of information

The College discloses information about its staff and students to the following:

Staff

Relevant government departments and other bodies to whom we have a statutory obligation to release the information, including:

- Department for Education
- Education and Skills Funding Agency
- Office National Statistics
- HMRC
- Department for work and pensions
- Potential employers of our staff

- Potential providers of education to our staff
- Pension Funds (Support staff – Merseyside Pension Fund; Teaching staff – Teachers Pensions')
- External agents employed by the College in the conduct its business e.g. HR & Payroll services provider, Disclosure and Barring service provider

Students
Relevant government departments and other bodies to whom we have a statutory obligation to release the information, including:

- Department of Education
- Education and Skills Funding Agency
- Office National Statistics
- Local Authorities
- Current or potential employers of our students
- Current or potential providers of education to our students
- Students former schools/colleges, for College 'alumni' purposes
- External agents employed by the College in the conduct of its business
- Work placement businesses

Restrictions on disclosure

Disclosures to persons or institutions not listed above nor in the data listings held by the College DPO, will only be made with the permission of the member of staff or student unless exception circumstances apply, as provided by law.

Appendix 5: Data held for Students and Data Retention

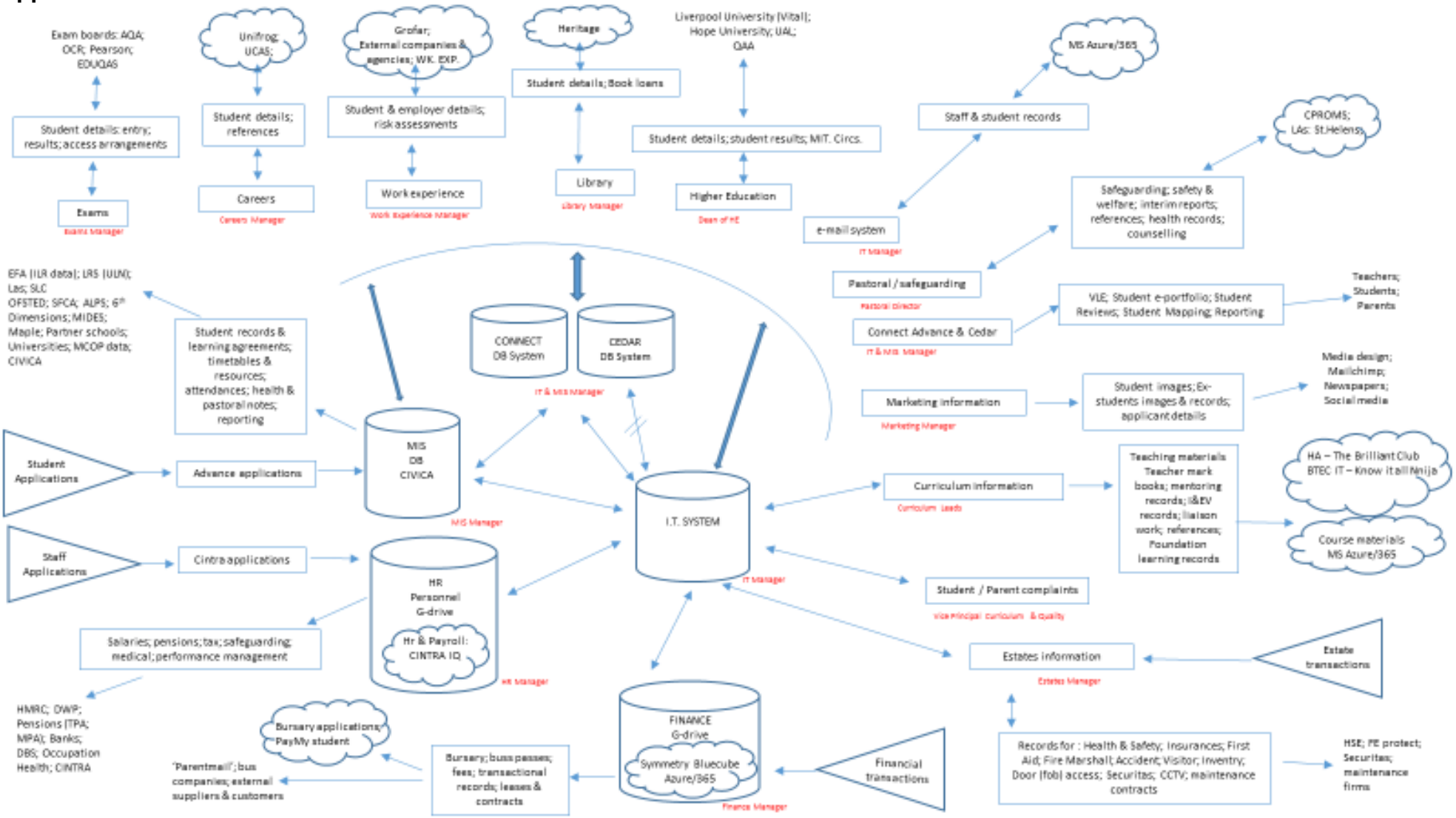
Student Data	Data processing necessity	Eventual data retention period
	To provide education under the education Act (1992); Safeguarding regulations apply to all; Limitation Act 1980c.58 to apply below as appropriate	
Core personal data including:	**For future career enquiries - identification of student presence at college, courses taken and grades. Permits the production of academic references for ex-students.**	**MIS retention In perpetuity. [College often has to provide academic information]**
Student full name		
Date of Birth		
Address		
Unique learner no & Student ref no		
Courses taken (with results, dates and exam board)		
Gender		
Previous School		
Personal data including:	**Limitation period for negligence. Permits College to provide comprehensive personal references for a stated period; Safeguarding regulations apply to all; Limitation Act 1980 c.58 to apply below as appropriate**	**MIS retention 6 years from end of course to apply below unless stated – then removed**
Ethnic Origin		
Disabilities		
Religion		
Learning difficulties	Equality Act 2010	
Country of domicile		
Qualification on entry		
Contact details (incl. phone & email)		
Next of kin		
Emergency contacts		
Application & Courses Applied for		Enrolling as above; Not enrolled - current academic year + 1 year
Reviews of progress		
Assessment marks		
Reasons for college absence		
Disciplinary matters		
Careers Advice		
Subject and personal tutor comments		
References (UCAS)		
References (other)		
Photograph		
In some cases:		
Family Income (bursary applicants)		
DBS details		
Health issues (incl. pregnancy)		

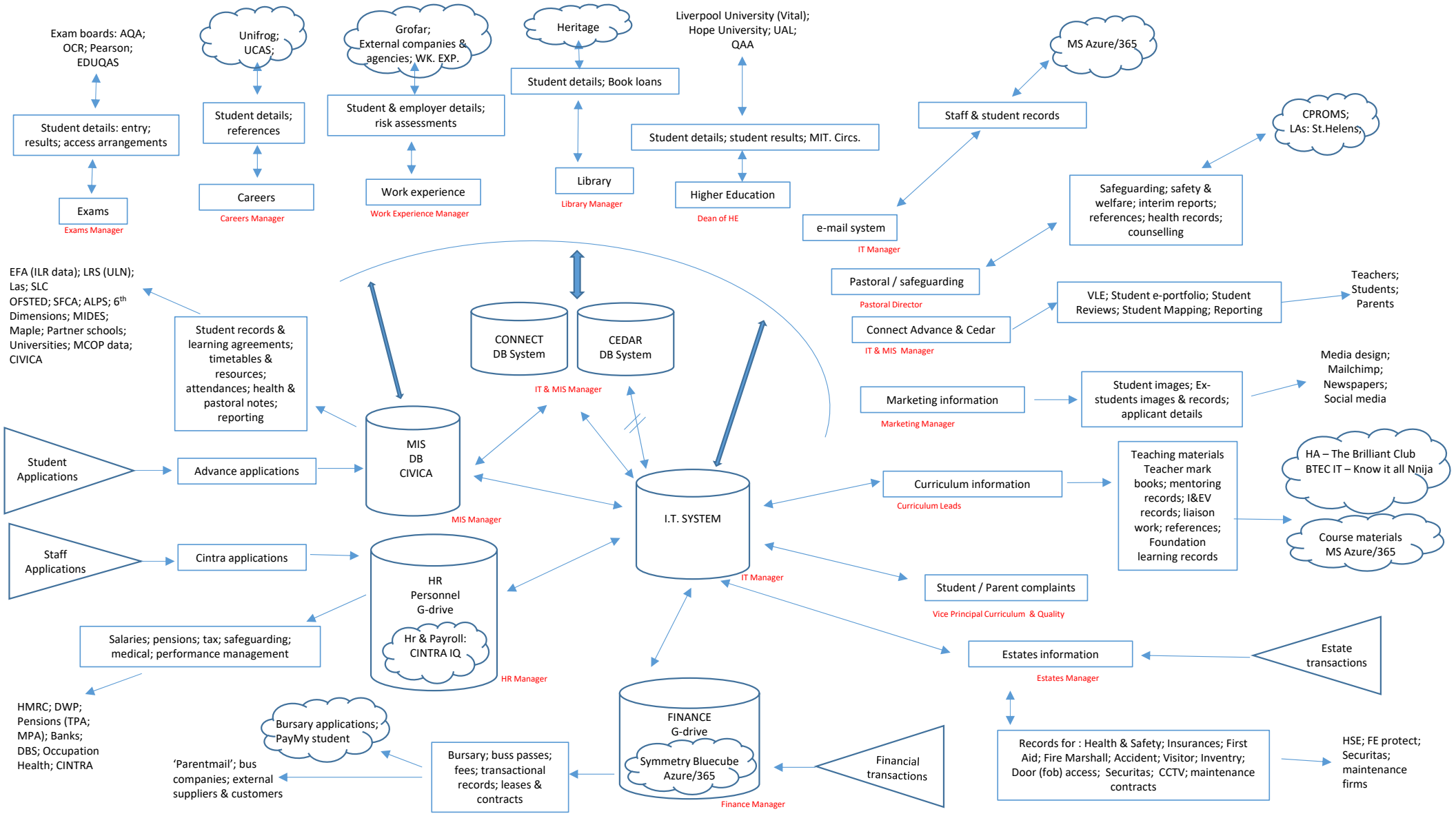
Appendix 6: HR Data for Staff / College and Data Retention

Staff Data	Data processing necessity and reason for length of retention	Eventual data retention period adopted
	All processed in accordance with: employment legislation, recruitment legislation, Equality and Diversity monitoring, health and safety legislation.	
Core personal data including:	**For future career enquiries - identification of staff presence at college. References and potential litigation. Limitation Act 1980 c.58 to apply below as appropriate**	**MIS retention (CIVICA from 2009 on-wards) in perpetuity. Materials prior to 2099 in archive.**
Staff full name		
Date of Birth		
Address		
Dates of employment		
Roles within College		
Contact details (incl. phone & email)		
Gender		
Ethnic origin		
Disabilities		
Religion (if declared)		
Holidays taken		
Absence period and reasons	General: Statutory Sick Pay Manual for employers CA 30.	Termination of employment + 40 years. Compassionate leave etc: current year+1yr
Personnel files and training records, disciplinary/grievance records, working time records.		
Performance management reviews		
Pension details		Termination employment +75years (or 100)
Income tax and NI returns, income tax records and correspondence with HMRC	S.I. 1993 / 744 * The Income Tax (Employments) Regulations 1993	
Records relating to Statutory Maternity /Adoption/ Paternity/ Shared Parental Pay	1992 c.4 Social Security Contributions & Benefits Act 1992; S.I. 1986 / 1960 * The Statutory Maternity Pay (General) Regulations 1986 (Amended by SI 729 2005)	
Statutory Pay & Maternity records, calculations, certificates (Mat B1s) or other medical evidence.	1994 c.23 Value Added Tax Act 1994; IR CA30 Statutory Sick Pay Manual for employers CA30;	
Statutory Maternity Leave entitlements	The Maternity & Parental Leave Regulations 1999 S.I. 3312;	
Wages and salaries including overtime, bonuses, and expenses	1970 c.41 Equal Pay Act 1970; S.I. 1999 / 584 * The National Minimum Wage Regulations 1998; 1970 c.9 * 1970 c.9 Taxes Management Act 1970	
Next of Kin		
Emergency contacts		
Personal data including:	**References and potential litigation. Limitation Act 1980 c.58 to apply below as appropriate**	**Archive - retention 6 years from end of course to apply below unless stated – then removed**

Application forms and interview notes: DBS; Education & quals; employment history; references from employers; results of previous employment groups	Equality Act 2010	unsuccessful – 6 months after application; successful - transferred to personnel file
Absence periods and reasons for absence	General: Statutory Sick Pay Manual for employers CA 30.	Termination of employment + 40 years. Compassionate leave etc: current year+1yr
Statutory Pay & Maternity records, calculations, certificates (Mat B1s) or other medical evidence.	1994 c.23 Value Added Tax Act 1994; IR CA30 Statutory Sick Pay Manual for employers CA30;	
Health issues (including pregnancy)	Health and Safety at Work etc. Act 1974	
Medical & Health records where termination of employment is related to Control of Hazardous Substances or to asbestos related illnesses.	Health & Safety at Work etc. Act 1974 C.37. The Control of substances Hazardous to health regulations 2002 S.I. 2677 The Control of Asbestos at Work regulations 2002 267	Stored in Estates Termination of employment + 40 years. Also for major injury arising for accident in the workplace. Termination of employment + 40 years. Also for major injury arising for accident in the workplace.
Photograph		Stored in IT

Appendix 7: Schematic data chart




Exam boards: AQA; OCR; Pearson; EDUQAS
Student details: entry; results; access arrangements
Exams
Exams Manager
Unifrog; UCAS;
Student details; references
Careers
Careers Manager
Grofar; External companies & agencies; WK. EXP.
Student & employer details; risk assessments
Work experience
Work Experience Manager
Heritage
Student details; Book loans
Library
Library Manager
Liverpool University (Vital); Hope University; UAL; QAA
Student details; student results; MIT. Circs.
Higher Education
Dean of HE
MS Azure/365
Staff & student records
e-mail system
IT Manager
CPROMS; LAs: St.Helens;
Safeguarding; safety & welfare; interim reports; references; health records; counselling
EFA (ILR data); LRS (ULN); Las; SLC
OFSTED; SFCA; ALPS; 6th Dimensions; MIDES; Maple; Partner schools; Universities; MCOP data; CIVICA
Student records & learning agreements; timetables & resources; attendances; health & pastoral notes; reporting
CONNECT DB System
CEDAR DB System
IT & MIS Manager
Pastoral / safeguarding
Pastoral Director
Connect Advance & Cedar
IT & MIS Manager
VLE; Student e-portfolio; Student Reviews; Student Mapping; Reporting
Teachers; Students; Parents
Marketing information
Marketing Manager
Student images; Ex-students images & records; applicant details
Media design; Mailchimp; Newspapers; Social media
Student Applications
Advance applications
MIS DB CIVICA
MIS Manager
I.T. SYSTEM
IT Manager
Curriculum information
Curriculum Leads
Teaching materials Teacher mark books; mentoring records; I&EV records; liaison work; references; Foundation learning records
HA – The Brilliant Club BTEC IT – Know it all Nnija
Course materials MS Azure/365
Staff Applications
Cintra applications
HR Personnel G-drive
Hr & Payroll: CINTRA IQ
HR Manager
Student / Parent complaints
Vice Principal Curriculum & Quality
Salaries; pensions; tax; safeguarding; medical; performance management
HMRC; DWP; Pensions (TPA; MPA); Banks; DBS; Occupation Health; CINTRA
Estates information
Estates Manager
Estate transactions
Bursary applications; PayMy student
'Parentmail'; bus companies; external suppliers & customers
Bursary; buss passes; fees; transactional records; leases & contracts
FINANCE G-drive
Symmetry Bluecube Azure/365
Finance Manager
Financial transactions
Records for : Health & Safety; Insurances; First Aid; Fire Marshall; Accident; Visitor; Inventry; Door (fob) access; Securitas; CCTV; maintenance contracts
HSE; FE protect; Securitas; maintenance firms