Greenhead College Corporation

Data Protection Policy

Review June 2026

Policy Holder:	*Director of IT, Estates and Operations*
Date drafted:	*June 2026*
Date accepted by the Corporation:	*6/7/26*
Date Impact Assessed by Policy Holder:	*June 2026*
Date of next review:	*June 202*
To be reviewed by:	*Director of IT, Estates, & Operations*

"This policy has been impact assessed to ensure it complies with all aspects of Diversity and Inclusion. Members are reassured that this policy is compliant with current equality legislation".

1.0 Introduction

Greenhead College's Data protection and use of information policy sets out the principles for handling data responsibly and securely within our college. This policy is also related to data concerning natural persons about whom we hold data (data subjects) and is designed to fulfil the requirements of the General Data Protection Regulation (GDPR) that came into force in May 2018.

Schools & Colleges are obliged by law to fulfil the requirements of the GDPR and ensure that procedures are in place to satisfactorily assure that all areas of this policy are operating in practice.

In addition to this, the College is committed to ensuring that we have a safe data environment that respects the rights of all people that are affected by the scope of the GDPR and beyond. We will strive to continue making improvements in a changing data environment, and to challenge systems and individuals falling below the standards expected.

2.0 Data Protection principles

2.1 Data Protection legislation, consisting of the UK GDPR and the Data Protection Act 2018, are underpinned by six important principles. These say that data must:

- Be processed fairly and lawfully.
- Be processed for limited purposes and in an appropriate way.
- Be adequate, relevant and not excessive for the purpose.
- Be accurate and kept up to date.
- Not be kept longer than necessary for the purpose.
- Be secure.

2.2 Article 5(2) of the UK GDPR states that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2.3 Greenhead College will ensure compliance with the data protection principles in the following ways:

- Greenhead College recognises that it is a public authority, as defined by the GDPR and must take accountability for this data and use of information policy in this context. As such we recognise that we are accountable for the data we control and have a responsibility to ensure those that process our data do so in line with the GDPR requirements.

- Greenhead College is serious about maintaining the highest standards of data management, ensuring that all people on whom we hold data are treated with respect and their rights are understood and held in high regard.

- Greenhead College will monitor its data environment and ensure that all data that we control, or process is audited regularly and, if appropriate, assessment made as to the impact of data processing on our data subjects.

- Due regard will be given to the design of our systems, so as to ensure that the security of people's data is given high priority and that we will only hold data that is needed to lawfully and legitimately fulfil our organisation's operation. People within our organisation will only be given access to data that they need to carry out their roles and responsibilities at the college.

- We will uphold the rights of individuals to make legitimate requests for data, in a variety of categories as defined by the regulations and will respond to these requests reasonably and as laid out by the regulations.

- We will not hold data for longer than is reasonably needed and will dispose of time expired data in a suitable way given the level of sensitivity of the data.

- Greenhead College will ensure that the organisation has the necessary skills and support to respond to data requests, by having a suitably trained Data Protection Officer who will co-ordinate policy and procedures, respond to such requests and report to the Corporation Governing Body on progress against the requirements of the GDPR.

- Should any data breaches occur then these issues will be dealt with promptly and efficiently, as required by the GDPR, and Greenhead College will liaise with the Information Commissioner's Office (ICO), through the Data Protection Officer, and other agencies as directed in order to remedy these breaches and to learn lessons from any such breaches.

- Greenhead College will communicate with people that are classified as our data subjects (people about whom we hold data) and will inform them of what data we hold about them via privacy notices, what the lawful reason for holding this personal data is, and for how long we will hold the data. This is to ensure that our processes are transparent and that all people included in our data recording activities are treated fairly.

- Greenhead College will give training to all staff and other key stakeholders on data management, with regard to the scope of the GDPR and in order to ensure better data security, and to specific staff on the management of data where that is appropriate to their role. Refresher training for all staff will take place every two years.

- Should the standards we expect not be adhered to, accidentally or deliberately, then appropriate investigations will be conducted, recommendations made and remedial action taken, potentially including disciplinary action.

3.0 Our data

It will be the responsibility of Greenhead College to ensure that we have a clear understanding of any data that we hold with regards to our data subjects (as defined by the GDPR).

This data must be understood at a granular level and the reason for holding this data must be understood. Furthermore, a lawful reason for holding this data must be established and documented in order to ensure that our data subjects are protected from inappropriate use of their personal data and to minimise the risk of identity fraud.

An annual internal data audit will be conducted to ensure that:

- our data records are up to date
- these records are complete and accurate
- any new data systems or processes have been included and their impact assessed
- any data due for destruction has been destroyed securely
- all requirements of the GDPR are being met

When carrying out the audit, the following should be considered:

A. all characteristics that are held with relation to the data subject
B. whether special category data is held
C. how long the data should be held for
D. What the lawful reason for holding the data is
E. what system the data is held on
F. who is responsible for managing that data system

Following the audit, any work required to ensure that all aspects of this policy are complied with should be carried out without undue delay, or an action plan be put in place to close any identified gaps.

4.0 Definitions

The following are definitions as defined under the relevant data protection legislation:

- **Data Protection Laws** – The UK General Data Protection Regulation and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator including the Data Protection Act 2018.
- **DPO** – Data Protection Officer, assist the College to monitor internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects and Information Commissioner's Office (ICO).
- **ICO** – Information Commissioner's Office.
- **Data Subjects** – includes all living individuals about whom the College holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
- **Personal Data** – refers to any information relating to a living, identifiable person who can be directly or indirectly identified in particular reference to an identifier.

- **Data controllers** - A controller determines the purposes and means of processing personal data. In most cases, the College would identify itself as the data controller.
- **Data Processors** - includes any person or organisation who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers who handle personal data on our behalf.
- **Processing** - is any activity that involves the use of personal data. It includes obtaining, recording or holding data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- **ROPA** - Record of Processing Activity, a central database/inventory held by the College to manage all processing activities in line with the ICO accountability principle. This database is managed by the College DPO.
- **Special Category Data** – includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition, sexual life and/or sexual orientation, genetics and biometric information (where it is used for ID purposes). Special category data is personal data that is more sensitive, and so requires more protection.
- **Third party** – means a natural or legal person, public authority, agency or body other than the data subject or controller.

5.0 Compliance with the GDPR and managing information responsibly

As the data controller for our information Greenhead College has a number of responsibilities with regard to ensuring that our data is compliant with the requirements of the GDPR. We will ensure that these responsibilities are upheld by complying with the GDPR and more specifically putting the following processes in place:

- Undertaking a data audit on an annual basis (as above) in order to ensure that we understand the data that we hold at the College and have a record of our processing activities.

- Reviewing the design of our data to ensure that we are minimising the risk of data breaches, and that unnecessary data is not held in our systems

- Communicating with data subjects at least annually with reference to the data that we hold and why we hold it. This will be done through the issue of privacy notices which will be published on the College website.

- Following a documented process to manage all data requests received from our data subjects and other parties that may request information from our organisation. This process will ensure that all the rights of the individual as laid out in the GDPR are respected and that timescales are adhered to.

- Appointing a trained Data Protection Officer who will be responsible for co-ordinating and implementing the policy of the College. They will ensure compliance across all the colleges, report to the Governing Body on progress against the requirements of the policy and be the published contact point for requests for information. Refer to section 6 for more information.

- Contacting data processors in order to ensure that the requirements of the GDPR are in place. This will include, but is not limited to, information regarding the processing of data in international environments.

- Following a documented process to ensure that data breaches are recorded, and appropriate decisions are made about communicating with the ICO and the data subjects of any such breach.

- Establishing data retention periods for each element of data and ensuring that destruction /deletion of data is undertaken as required.

- Explaining clearly the way in which data is used by data users in our organisation. Each user of data will be asked to record their understanding of their responsibilities. An acceptable use statement has been prepared for different information users so that it is clear to them how to use data in an acceptable way as a part of our college community.

- Providing guidance, best practice and requirements for ensuring that online safety is promoted and monitored in college. This is done in the best interests of the whole college community and is be reviewed regularly in order to ensure that the impact of developing technologies is taken into consideration.

6.0 Artificial Intelligence

AI is a powerful tool that can be leveraged for learning, writing and research, but it is important that we use it ethically and responsibly both within the context of our College and with a view to the future.

We respect the privacy of users, and their data and so personally identifiable information (PII) is deemed off-limits for AI tools in College.

In line with the Data Protection Act (2018) and the methods AI tools use for storing data, the College will not upload PII in student work to AI platforms for the purpose of assessment.

The College's Acceptable Use Policy provides further information of what is deemed acceptable and unacceptable in the use of AI.

7.0 Personal Data Breach

7.1 A personal data breach means 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. This includes breaches that are the result of both accidental and deliberate causes. If a member of staff or student believes a breach has taken place, they should contact the Data Protection Officer immediately.

7.2 On becoming aware of a data breach a full investigation will be completed by the Data Protection Officer who will contain the situation, assess the potential adverse consequences for individuals, recover the breach if possible and report to the ICO where appropriate within 72 hours. Any individual affected by a significant breach will be informed including the measures taken to mitigate any possible adverse effects.

7.3 Any security incident will be investigated to determine if the breach was a result of human error, a system error or of a malicious nature. Further staff training and revisions to systems may take place as identified following the investigation. All staff are aware than any breach of the Data Protection Policy may result in the College's disciplinary procedures being instigated.

7.4 Actions to be taken in the event of a security breach can be found in Appendix D

8.0 Subject access requests

8.1 All individuals who are the subject of personal data held by the College are entitled to:

- Ask what information the College holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the College is meeting its data protection regulations.

If an individual contacts the college requesting information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at dpo@greenhead.ac.uk.

The college will always verify the identity of anyone making a subject access request before handing over any information.

In the first instance, all subject access requests should be forwarded to the Data Protection Officer (or designated individual acting in the role in their absence).

The college will reserve the right to take further steps to satisfy itself of the identity of anyone requesting data.

8.2 On receipt of a subject access request:

- The request will be logged on the Subject Access Request Log spreadsheet.
- The request will be initially assessed by the DPO to determine how the College should respond.

- A response acknowledging receipt of the request will be sent to the person requesting the data.
- Any data recovered will be dispatched in electronic form in the first instance. The data will be encrypted, and the encryption key will be dispatched separately. The college will seek to use an alternative communication channel to send this key eg via SMS to a known mobile phone number.
- The College will act to protect the data of data subjects at all times and may take further steps to establish confidence that the data is being sent to the person lawfully entitled to receive it before sending personal data.

9.0 Training and awareness

The training of staff and other users of data at Greenhead College will be given a high priority, to minimise the risk of inappropriate use of data, to minimise the risk of data breaches and promote the best practice in deliver the objectives of the College whilst respecting the rights of our data subjects.

Training will be given on a regular basis and will include different messages for different staff and users of data. Staff or other users of data that handle specific or special category data will be given further training as necessary to ensure that they are fully aware of the impact that they might have if data is not handled appropriately.

We will also promote awareness amongst the whole community of data users and data subjects alike to ensure that there is an awareness of the need for balancing the needs of the college in controlling and processing personal data with the rights of individuals in protecting their own data.

10.0 Review

Our data environment is extremely dynamic meaning that review of our approach to information systems must remain under review and keep up to date with recent developments. This will mean that this policy will be updated at least annually and the schedules that inform the procedures that are in place for specific elements of our policy will be updated to reflect best practice and changing regulations.

11.0 Additional Information

- Acceptable use of ICT documents for data users – refer to the ICT and internet acceptable usage policy and information security guidance on the college website
- Data audit template and record of processing activity – Held by the Data Protection Officer dpo@greenhead.ac.uk – to be completed annually.
- Data impact Assessment – Held by the Data Protection Officer dpo@greenhead.ac.uk – to be completed on purchase of new information systems.
- Privacy notices – refer to the Privacy notices on the college website
- Information request procedure – Refer to the Freedom of information policy on the college website

- Data Breach Procedure – Held by the Data Protection Officer
- Data retention periods – Refer to Appendix B and Disposals Policy
- Detailed DPO job description – Refer to Appendix A
- Online safety guidance – Refer to the ICT and internet acceptable usage policy and information security guidance on the college website
- Data user and stakeholder responsibilities – Refer to Appendix C

APPENDIX A

Role Description: Data Protection Officer (DPO)

Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the college's data protection processes and advise the College on best practice.

Key responsibilities

To:

- Advise the college and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the college's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the college's compliance with data protection law, by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to the college leadership team
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the college's policies are followed, through:
    - Assigning responsibilities to individuals
    - Awareness raising activities
    - Co-ordinating staff training
    - Conducting internal data protection audits
- Advise on and assist relevant college staff with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example staff, students and parents / carers), including:
    - Responding to subject access requests
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focussing on these
    - Advising the college principle if/when it should conduct and audit, which areas staff need training in, and what the DPO role should involve
- Report to the governing body on the data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role

- Undertake any additional tasks necessary to keep the college compliant with data protection law and be successful in the role.
- Maintain a record of the College's data processing activities
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues
- Take responsibility for fostering a culture of data protection throughout the college
- Work closely with other departments to ensure GDPR compliance, such as HR, IT etc

Appendix B: Data retention - Schedule and Guidance

The College take care to store data for a period of time that reflects their needs but equally protects the rights of individuals. However, there are still legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to education, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and
- the General Data Protection Regulation (from May 25th 2018).

These inform not only retention periods, but also what to keep and who should be able to access it.

On 25th May 2018, the General Data Protection Regulation came into effect across the UK.

Introduction

Reasons to keep certain records, such as child protection records, for many years after students or staff leave the College need to be weighed against personal rights and be supported by a lawful reason. Longer retention of data, particularly special category data mean that the college will put in place more secure storage systems and protocols in place.

The College takes steps to ensure its retention policies are communicating the reasons for the policy in privacy notices and staff or parent/carer contracts and are ensuring any records necessary to keep long term are kept very secure, accessible only by trained staff who require this information to perform their official function.

Personal data is kept for a period of time as defined below, with statute for the retention of records being a key factor in many decisions in the length of retaining data. Annual data review schedules are undertaken to ensure that records no longer required are disposed of appropriately.

1. Archiving and the disposal or erasure of Records

All staff receive basic training in data management – issues such as security, recognising and handling personal data, safeguarding etc. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- That records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required;
- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether data sticks, personal servers / data storage or mobiles and handheld electronic tablets) unless

absolutely necessary, in which case it should be subject to a risk assessment and in line with an up-to-date IT acceptable use policy;
- That questions of back-up or migration are likewise approached in line with general college policy (such as professional storage solutions or IT systems) and not individual ad hoc action;
- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements providing for security and access;
- That information storage systems will, over time, be enhanced to allow erasure of records to be more efficient and granular over time. This will form part of review processes on a periodic basis;
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to date); and
- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.
- This is particularly important in respect of the College's specific legal obligations under the GDPR. However, they amount to common sense rules even where personal data is not directly involved. This is also supported by our acceptable use of ICT policy.

2. Retention periods

Consideration is given as to how long each category of record should be kept. In particular, statutory guidance will be taken into account with regard to particular types of record (e.g. Safeguarding information, financial invoices) to ensure that the College is able to have a strong organisational memory that allows us to recall vital information.

The Schedule below is guided by these principles and where there is no statutory guidance is in place the data is be held to support our organisational memory with respect to key decisions, balancing this with the rights of individuals.

In some cases the prompt for disposal may be the end of a calendar year or financial year, meaning that disposal dates will not be exact and the annual cycle of activity will need to be taken into consideration.

Should the College have particular reasons for retaining data beyond the periods laid out in the schedule (e.g. pending court action / ongoing investigation) then periods may be extended, supported by evidence to validate that decision.

3. Recording information

All staff must be clear, when creating documents and records of any sort (including email), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request under the GDPR. All records must be, amongst other things, be accurate, clear, professional and objective.

4. Secure disposal of documents

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Where third party disposal experts are used they should ideally be supervised but, in any event, be under adequate contractual obligations to the College to process and dispose of the information securely.

5. Rules applicable to child protection (CP) files

Often CP files will comprise personal, special category or sensitive personal data (e.g. physical or mental health, sexual life or criminal allegations). Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a GDPR perspective, make it easier for a college to justify retention for long periods – even the lifetime of former staff and students.

- Child protection concerns, disclosures, referrals, etc relating to individual students must be recorded, stored and maintained as described in 'Keeping children safe in education' (DfE 2016) – no child protection / safeguarding information should be recorded in a student's educational records;
- The CP files must be stored in a locked cabinet or – if electronic – in a secure format, with controlled access only to the Designated staff and Principal. If the records need to be viewed by another person (e.g. a member of pastoral staff, inspector, police) a record should be made on the chronology of the date, the identity of the person and the purpose;
- If using an electronic CP recording system, the provider must give assurances that the appropriate security certificates are in place. Staff should not pass cause for concern notifications to the DSL via email but via the designated system;
- Each student should have their own file; no "family" files should be kept. The front of the file should include a sheet detailing contact details of those with parent/carer rights, other significant adults in the household, any allocated social worker or other agencies involved, etc. Each file should also include a chronology of key events;
- If a student leaves college to move to another sixth form or an FE college, the CP file should be transferred securely to the new Designated Safeguarding Lead as soon as possible. Ideally this will be by face to face handover (with electronic files being via a secure transmission protocol); if it is necessary to post the file this should be by secure mail and the new DSL should be notified to expect it. A copy should be retained by the college however, and archived in the manner below;
- When a student leaves the college for any reason, the CP file should be archived in line with the following retention schedule:
    - If the file contains low level concerns that have never led to a referral to partner agencies – retain until the student's 25th birthday (or the end of that academic year);
    - If a referral was ever made to children's social care or the student is or has been looked after – review retention of the record to reflect the need for that record based on potential risk to the student;
- In the event that a parent/carer or student requests sight of the CP file the college should seek advice from the Principal and Data Protection Officer without delay. Parent/carers do not always have an automatic right to access their child's personal information under a Subject Access Request: if the student is old enough to make the decision (determined to be the age of 13), then it is the student's decision whether his or her parent/carers should exercise the right under data protection law to access his or her personal data.

- It is within the protocols of handling this data that information pertinent to a student should be handed over (with a secure audit trail) to the student's next educational establishment thus avoiding duplication of records and further risk of data breach.
- Please note that IICSA (Independent Inquiry into Child Sexual Abuse) has issued very strong guidelines on not destroying or deleting files which may be of interest to the Inquiry, whether or not a college has received a letter from IICSA. How a college handles records and concerns raised may be within the scope of the Enquiry, even if there was no major incident. It is expected that the final report produced by IICSA will contain recommendations about recording, retention and storage that may become law but until then a cautious approach to retention is advisable.

TABLE OF RETENTION PERIODS

Type of Record/Document	Retention Period
COLLEGE-SPECIFIC RECORDS	
Registration documents of College	Permanent (or until closure of the college)
Attendance Register	6 years from last date of entry, then archive.
Minutes of Governors' meetings	10 years from date of meeting
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL STUDENT RECORDS	*NB – this will generally be personal data*
Admissions: • *Admission file* • *Admission appeals*	1 year after student leaving college
Attainment • *Attainment data, test results*	5 years after student leaving college
Attendance data	5 years after student leaving college
Record of absence	1 year after student leaving college
Record of exclusion	1 year after student leaving college (transferred to new setting with transfer file)
Behaviour information • *General Behaviour incidents*	1 year after student leaving college (transferred to new setting with transfer file)
Trips and activities • *Trip information, consent and visitors record*	Immediately after trip or visit
Financial records from trip	6 years in line with other financial records
Record of major incidents	Until student reaches age of 25 (subject to individual case risk assessment)
Medical information • *Permission to administer medicine*	1 month after end of medication being administered
Medical conditions and ongoing management	1 year after student leaving college
Serious medical incidents	Until student reaches age of 25 (subject to individual case risk assessment)

Safeguarding records (to be risk assessed individually) A. *Safeguarding records with no referrals to other agencies* B. *Safeguarding records referred to other agencies* C. *Safeguarding records of Children that have been looked after*	A. 5 years from date of record B. Minimum 25 years from date of birth then undertake risk review C. Minimum 25 years from date of birth then undertake risk review *Note that these records should be passed on (with a verification of handover) to the next environment in which the child is being educated – no personal data records should be retained in the college after the child has left*
SEN records • *Records of Special Educational needs*	25 years from date of birth *Note that these records should be passed on (with a verification of handover) to the next environment in which the child is being educated – no personal data records should be retained in the college after the child has left*
Other student information A. *Photographic identifier in Management information System (for identification)* B. *Other photographic information (e.g. for publicity / social media)* C. *Name and Address* D. *Student characteristic information* E. *Parent/carer contact and status information* F. *Biometric information (if held)*	A. 1 year after student leaving college B. In line with specified consent C. 1 year after student leaving college D. 1 year after student leaving college E. 1 year after student leaving college F. In line with consent (whilst data is actively in use)
SAFEGUARDING	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
Child Protection files	Low level concerns, no multi-agency act - 25 years from date of birth; for other instances see above

FINANCIAL RECORDS	
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state e.g. invoices / VAT records etc.)	6 years from the end of the financial year in which the transaction took place
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
Insurance records	Minimum – 7 years
CONTRACTS AND AGREEMENTS	
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
EMPLOYEE / PERSONNEL RECORDS	*NB this will almost certainly be personal data*
Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken. For former staff this will be in their employment file, for current staff this will be in the SCR.
Contracts of employment	7 years from effective date of end of contract
Employee appraisals or reviews	7 years from effective date of end of contract
Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims. Allegations of abuse will be kept for 10 years or to retirement age whichever is longer
Payroll, salary, maternity pay records	6 years
Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
Immigration records	4 years
Health records relating to employee	7 years from effective date of end of contract

ENVIRONMENTAL & HEALTH RECORDS	
Accidents to children 25 years from birth (unless safeguarding incident)	25 years from birth (additional review for safeguarding incidents)
Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case
Staff use of hazardous substances	7 years from end of date of use
Risk assessments	7 years from completion of relevant project, event or activity.
Asbestos register and plan	Permanent

Note: all records are subject to review prior to destruction and any records being retained will be accompanied by a documentary justification for additional retention.

All records will be disposed of in line with the College Disposals Policy.

APPENDIX C - Key responsibilities

Introduction

We all have responsibilities for protecting personal data and using information responsibly. To ensure that this happens on a consistent basis throughout our organisation this will be made clear to all that are part of our data ecosystem, and specific responsibilities will be given to ensure there is clarity around accountability and responsibility for particular areas of implementing the policy.

The responsibilities of the various parties affected by this policy are as follows:

A. Corporation Governing Body

The Governing Body of Greenhead College is ultimately responsible for ensuring that the Data protection and use of information policy in place complies with the General Data Protection Regulation and satisfies other guidance relating to the use of information in colleges.

They will monitor the policy and ensure recommendations and reports submitted to them by the ICO or Data Protection Officer are given due consideration and action taken as necessary.

The Governing Body will receive information regarding any data breaches and information requests relating to the College during the course of the year and ensure that action is being taken to maintain high standards of data management.

The Governing Body will review the data protection policy and its schedules on a periodic basis to ensure that the policy remains coherent and up to date.

The Governing Body will also be asked to ensure the oversight of the implementation of any actions as agreed at meetings from time to time.

The Governing Body will be responsible for appointing the Data Protection Officer

B. The Data Protection Officer

The Data Protection Officer has specific responsibilities laid out in the General Data Protection Regulation. The principles of these are laid out below:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, students / parent/carers, customers etc).

In carrying out these responsibilities, the Data Protection Officer will report to the Governing Body and submit reports and recommendations regarding the operation of the policy. The

Governing Body will ensure that the Data Protection Officer is protected from any disciplinary action with regards to carrying out their duty with regards to the GDPR.

The Data Protection Officer will be appointed and will work under the direction of the Governing Body, having access to inform this decision making body directly.

The Data Protection Officer will provide support and documentation to the relevant staff in order to ensure that the administrative processes associated with GDPR and data management are as clear as possible.

C. **Third- party data processors**

Where external companies are used to process personal data on behalf of the college, accountability for the security and appropriate use of that data remains with the college and ultimately the Governing Body.

Where a third-party data processor is used:

- a data processor must be chosen providing sufficient guarantees and evidence about its ability to protect the personal data of the data controller's data subject.
- reasonable steps must be taken that such security measures are in place, including written or contractual evidence that data security measures are in place with regards to relevant data.
- Further assurances regarding data processed outside of the United Kingdom must be sought in order to ensure that appropriate security is in place for the processing of this data.

D. **Students accessing data**

Students will be given clear guidance on the acceptable use of information within their college life. It is their responsibility to adhere to these guidelines and ensure that they follow the college's guidance in this area.

They are expected to adhere to all of this guidance and any breaches will be investigated and further action may be taken.

Further details of what their responsibilities with regard to this can be found in the Acceptable use of IT schedule.

E. **Staff**

Staff and other users may be given access to data and use this in the course of doing their work or employment. It is their responsibility to ensure that data that they have access to will be treated within the guidelines outlined. Each of these individuals will be given training on the use of data and protecting the rights of data subjects. Failure to comply may result in disciplinary action against the individual.

F. **Other users of information**

Other users of information in the college must be given guidance on what information they are able to access. This will be designed to absolutely minimise access to personal data and will be within a clearly defined lawful reason, supported by a data sharing agreement where appropriate. When being given access to this information the college will monitor that this information is the only information being accessed. It is the responsibility of these users to access only the information agreed and misuse of information will lead to corrective action up to and including legal action and remedies.

Greenhead College Corporation

Impact Assessment

Data Protection Policy

Reviewed June 2026

Policy Holder:	*Director of Estates and Operations*
Date Impact Assessed by Policy Holder:	*June 2026*
Date of next review:	*June 2027*
To be reviewed by:	*Director of Estates, Operations & IT*

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)

Policy title:	Data Protection Policy
Policy owner:	Sarah Walters Director of Estates and Operations
Date of latest review if applicable:	July 2025

EIA Date: June 2024

Main aims and purpose of the policy:

This policy has been written in accordance with The Data Protection Act 2018 which is the implementation of the General Data Protection Regulation (GDPR) and came into effect in May 2018. This policy and the way in which Greenhead College (the College) manages data protection is based upon the six principles defined in the Act. This policy also includes exceptions to rules such as The Education and Skills Act 2008 – Section 72 which allows the sharing of certain information between the educational establishment and the Local Authority.

Type of policy connect to EIA:

- **Proposed new policy**
- **Undertaking a review of an existing policy**
- **Other (please state):**

Please identify any potential impacts that the policy or development of this policy could have, on any of the equality grounds identified below.

Equality Ground	Identified Impact
Age	The policy is consistent in its approach to the management of the data protection policy regardless of age.
Disability	The policy is consistent in its approach to the management of the data protection policy regardless of disability.
Gender (including gender identity)	The policy is consistent in its approach to the management of the data protection policy regardless of gender.
Marriage and civil partnership	The policy is consistent in its approach to the management of the data protection policy regardless of marital or civil partnership status
Pregnancy and maternity	The policy is consistent in its approach to the management of the data protection policy regardless of whether a person is pregnant or on maternity leave.
Race	The policy is consistent in its approach to the management of the data protection policy regardless of race.
Religion or belief	The policy is consistent in its approach to the management of the data protection policy regardless of religion or belief.
Sex	The policy is consistent in its approach to the management of the data protection policy regardless of sex.

Sexual Orientation	The policy is consistent in its approach to the management of the data protection policy regardless of sexual orientation.
Social / Health Inequalities	The policy is consistent in its approach to the management of the data protection policy regardless of social status/health inequalities.

Select one of the four outcomes below to indicate how the development/implementation of the policy will be progressed and state the rationale for the decision.

Outcome 1: No change required – the assessment is that the policy is/will be robust and/or promotes Diversity and Inclusion. ■

Outcome 2: Adjust the policy – this involves taking steps to address any adverse impacts before the policy has been developed. ☐

Outline these steps:

Outcome 3: Continue the policy while mitigating against any potential adverse impacts. ☐

Outline how these adverse impacts can be mitigated against:

Outcome 4: Immediate referral to SLT/Governors, as there are adverse effects which cannot be prevented or mitigated against. ☐

Details of further steps (if required)	