GDPR Policy

Role	Review Criteria	Sign Off Date
Head of Technical College **Claire Oliff**	Data Controller (Owner)	19/01/2026
Technical College Operations Manager **Paul Stone**	Data Controller (Lead)	
Apprentice Delivery Manager **Chris Pape**	Data Controller (Lead)	
Apprentice Coordinator **Coral Violet**	Data Processor	
Human Resources Director **Gabrielle Zeter**	Policy Reviewer	19/01/2026
IT & Innovation Manager **Mark Walker**	Policy Reviewer	19/01/2026

Version	Date	Revision Author	Summary of Changes
0	20/05/24	Mark Walker	Initial document creation
1	25/05/24	Mark Walker	Minor adjustments to roles & responsibilities
2	19/01/2026	Claire Oliff	Minor formatting amendments, changes to staff roles to add clarity and change of 'pupil' to 'student'

1.0 Policy Statement

This General Data Protection Regulation (GDPR) policy outlines the responsibilities, procedures, and practices that KLM UK Engineering Technical College follows to ensure compliance with the GDPR regarding the processing and protection of personal data. This policy applies to all personal data collected, processed, and stored by KLM UK Engineering Limited, including data pertaining to students, staff and other stakeholders.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.1 Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on current guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

This policy also meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data in schools.

1.2 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything that is done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing may be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, who processes personal data on behalf of the data controller.
Data Protection Leads	Technical College Operations Manager & Apprenticeship Delivery Manager
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

2.0 Application

This policy applies to all employees, contractors, and third-party service providers who have access to personal data processed by KLM UK Engineering Limited. Staff who do not comply with this policy may be subject to disciplinary action.

3.0 Roles and Responsibilities

The Data Controller

KLM UK Engineering Technical College processes personal data relating to students, staff, visitors, and others, and therefore is a data controller.
KLM UK Engineering Technical College is registered with the ICO and will renew this registration annually or as otherwise legally required.

The Board of Directors

The Board of Directors of KLM UK Engineering Limited has overall responsibility for ensuring it complies with all relevant data protection obligations.

The Head of the Technical College

The Head of the Technical College is responsible for overseeing the implementation of this policy, monitoring KLM UK Engineering Technical College compliance with data protection law, and developing related policies and guidelines where applicable.
In collaboration with the HR Team, The Head of the Technical College will provide an annual report of activities directly to the Board of Directors and, where relevant, report to the board advice and recommendations on data protection issues.

The Head of the Technical College is the point of contact with the ICO and will offer advice and guidance to data protection leads.

Technical College Operations Manager and Apprenticeship Delivery Manager

The Technical College Operations Manager and Apprenticeship Delivery Manager act as the Data Protection Leads and support the data controllers on a day-to-day basis.

All Technical College employees are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy.
- Ensuring that any personal data they provide to the college (for example, their contact details) is accurate.
- Informing the college of any changes to their own personal data, such as a change of address.
- Being mindful of the fact that individuals have the right to see their 'personal data'. Therefore, employees should not record comments or other data about individuals, which they would not be comfortable in the individual seeing, either in emails or elsewhere.
- Not covertly or without permission recording (video or audio) students, staff, or other individuals.
- Only ever obtaining or using personal data relating to third parties for approved work purposes.
- Taking appropriate initial action to minimise the impact of a potential data breach. e.g., if an email containing personal data has been sent to an incorrect recipient, the email must be recalled immediately, and the college Data Protection Lead and IT informed.
- Contacting the college Data Protection Lead in the first instance in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.

- If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.
- If they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).
- If they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed. For example, if their laptop is stolen or their phone is lost, and it has personal data stored on it.

4.0 Linked Policies

This policy should be read in conjunction with the Technical College Safeguarding and IT and Communications policies.

5.0 Collecting personal data

5.1 Lawfulness, fairness, and transparency

Personal data will only be processed, where one of 6 'lawful bases' (legal reasons) exists to do so under data protection law:

- The data needs to be processed so that KLM UK Engineering Limited - Technical College can fulfil a contract with the individual, or the individual has asked KLM UK Engineering Limited - Technical College to take specific steps before entering a contract.
- The data needs to be processed so that the KLM UK Engineering Limited - Technical College can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g., to protect someone's life.
- The data needs to be processed so that the KLM UK Engineering Limited, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of KLM UK Engineering Limited - Technical College or a third party (provided the individual's rights and freedoms are not overridden).

For special categories of personal data, we will also meet one of the special category conditions under data protection law.

- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security, or social protection law.
- The data need to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise, or defence of legal claims.
- The data needs to be processed of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposed and the processing is done by or under the direction of a health or social work professional or by any other person obliged to confidentiality under law.

- The data needs to be processed for archiving purposes, scientific or historical research purposes or statistical purposes and the processing is in the public interest.

For criminal offense data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

5.2 Limitation, minimisation, and accuracy

- Personal data will only be collected for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when their data is first collected.
- If KLM UK Engineering Limited - Technical College wishes to use personal data for reasons other than those given when it was first obtained, the individuals concerned will be informed before this takes place, and consent sought where necessary.
- Staff must only process personal data where it is necessary to do their jobs. When staff no longer need the personal data they hold, they must ensure it is appropriately deleted. This will be done in accordance with KLM UK Engineering Limited - Records GDPR matrix.
- KLM UK Engineering Limited - Technical College will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate in relation to the KLM UK Engineering Limited GDPR matrix.

5.3 Sharing personal data

Personal data will not normally be shared with any other parties. However, exceptions to this are where:

- There is an issue that puts the safety of KLM UK Engineering Limited's staff or students at risk.
- KLM UK Engineering Limited - Technical College need to liaise with other agencies. If required, consent will be sought in advance.
- KLM UK Engineering Limited - Technical College or individual suppliers or contractors need data to enable the provision of services to our staff and pupils – for example, IT companies. When doing this, KLM UK Engineering Limited - Technical College will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data that is shared.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with KLM UK Engineering Limited

Engineering Limited - Technical College will also share personal data with law enforcement and government bodies where there is a legal requirement to do so, including for instance:

1.1.1 The prevention or detection of crime and/or fraud

1.1.2 The apprehension or prosecution of offenders

1.1.3 The assessment or collection of tax owed to HMRC

1.1.4 In connection with legal proceedings

1.1.5 Where the disclosure is required to satisfy our safeguarding obligations

1.1.6 Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided

KLM UK Engineering Limited - Technical College may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of the KLM UK Engineering Limited's students or staff.

Where personal data is transferred to a country or territory outside the European Economic Area, this will be done in accordance with data protection law.

6.0 Subject access requests and other rights of individuals

6.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that is held about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the school data protection lead and copied to the Head of Technical College. Requests should include:

1.1.7 Name of individual
1.1.8 Correspondence address
1.1.9 Contact number and email address
1.1.10 Details of the information requested

If staff receive a subject access request, they must immediately forward it to the college's data protection lead and the Head of Technical College.

6.2 Responding to subject access requests

When responding to requests:

- The individual may be asked to provide two forms of identification.
- The individual may be contacted via telephone to confirm the request was made.
- KLM UK Engineering Limited - Technical College will respond without delay and within one month of receipt of the request.

- The information will be provided free of charge.
- If the request is complex or numerous, the individual may be told that we will comply within three months of receipt of the request. The individual will be informed of this within one month and provided with an explanation of why the extension is necessary.

Information may not be disclosed if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the student is being or is at risk of abuse, but only in situations where the disclosure of such information would not be in the student's best interests
- Includes another person's personal data, unless such personal data can be reasonably anonymised or the person whose personal data is included provides consent to their data being disclosed.
- Is given to a court in proceedings concerning the student
- Forms part of sensitive documentation, including but not limited to those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential, or exam scripts

If the request is unfounded or excessive, KLM UK Engineering Limited - Technical College may refuse to act on it or charge a reasonable fee which considers administrative costs. See guidance from the ICO on where charges may be applicable. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.
When a request is refused, the individual will be provided with the reasons for the refusal and informed of their right to complain to the ICO

6.3 Parental requests to see the educational record

There is no automatic parental right of access to the educational record in academies, including free schools. If a parent wishes access to the educational record, then they should follow the subject access request process as set out in section 9.

7.0 Photographs and videos

As part of KLM UK Engineering Limited - Technical College activities, photographs may be taken, and images recorded of individuals. Written consent will be obtained from students, for photographs and videos to be taken of them for communication, marketing, and promotional materials. We will clearly explain to the students how the photograph and/or video will be used.

Uses may include:

- KLM UK Engineering Limited - Technical College notice boards, magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the company photographer, newspapers, campaigns.
- Online on the school or KLM UK Engineering Limited - Technical College or social media pages

Consent can be refused or withdrawn at any time. Where consent is withdrawn it may not always be possible for KLM UK Engineering Limited - Technical College to remove all images of the student from communication, marketing, and promotional materials.

CCTV is in operation at base maintenance at KLM UK Engineering. When students and staff are at this site, they will be subject to this and should consult the CCTV Policy on SharePoint for more information.

8.0 Data security and storage of records

- Personal data will be protected and kept safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. Members of staff must read and adhere to General Information Security Policy in relation to the security of electronic records.
- Employees should take appropriate steps to ensure the security of paper records for example, through locking away confidential papers when not in use, and ensuring confidential data is not left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. Staff and students, who store personal information on their personal devices must follow the same security procedures as for school-owned equipment.
- All staff, students, governors and volunteers must abide by this Data Protection Policy as well as KLM UK Engineering Limited's other policies including the General Information Security Policy.
- Where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Where personal information needs to be taken off-site, staff must sign it in and out from the school office.

9.0 Disposal of records

Personal data that is no longer needed will be disposed of securely. For further details, see KLM UK Engineering Limited's GDPR matrix.

10.0 Personal data breaches

KLM UK Engineering Limited - Technical College will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the procedure set out in appendix 1 will be followed.

- When appropriate, data breaches will be reported to the ICO within 72 hours.

Such breaches may include, but are not limited to:

- The theft of a KLM UK Engineering Limited - Technical College laptop containing non-encrypted personal data about pupils.
- Safeguarding information being made available to an unauthorised person.

10.1 Training

All staff will be provided with e-learning data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or KLM UK Engineering Limited - Technical College processes make it necessary.

11.0 Monitoring and reviewing our policy and practice

The Head of Technical College is responsible for monitoring and reviewing this policy with the Policy Reviewers. This policy will be reviewed and updated if necessary.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify KLM UK Engineering Limited - Technical College data protection lead.
- KLM UK Engineering Limited - Technical College data protection lead will immediately inform the Head of the Technical Training College.
- The Head of Technical College will investigate the report and determine whether a breach has occurred. To decide the Head of Technical College will consider whether personal data has been accidentally or unlawfully.
    - Lost e.g. Lost Laptop
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Head of Technical College will alert the Managing Director, HR Director, Director of Finance, and all necessary individuals.
- The Head of Technical College will make all reasonable efforts to contain and minimise the impact of the breach, assisted by other relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).
- The Head of Technical College will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Head of Technical College will work out whether the breach must be reported to the ICO. This will be judged on a case-by-case basis. To decide, the Head of Technical College will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation o Loss of confidentiality o Any other significant economic or social disadvantage to the individual(s) concerned If it is likely that there will be a risk to people's rights and freedoms, the Head of Technical College will notify the ICO.
- The Head of Technical College will ensure that the decision is documented by the data protection lead in KLM UK Engineering Limited - Technical College service management tool in case it is challenged later by the ICO, or an individual affected by the breach.
- Where the ICO must be notified, the Head of Technical College will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Head of Technical College will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Head of Technical College
    - A description of the likely consequences of the personal data breach o A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Head of Technical College will report as much as they can within 72 hours and submit the remaining information as soon as possible.
- The Head of Technical College will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Head of Technical College will promptly

inform, in writing, all individuals whose personal data has been breached. This notification will set out:

  - The name and contact details of the Head of Technical College
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The Head of Technical College will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies
- The Head of Technical College will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored by the Head of Technical College on KLM UK Engineering Limited service management tool.
  - The Head of Technical College and all other necessary individuals will review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving risky or sensitive information. We will review the effectiveness of these actions and amend them, if necessary, after any data breach.

Appendix 2: Definition of a breach

Under the General Data Protection Regulation (GDPR) in the UK, a data breach is defined as any incident where there is unauthorized access to personal data, its loss, destruction, alteration, or disclosure. Here are the key components of a data breach under GDPR:

Unauthorized Access: Any instance where individuals or systems gain access to personal data without authorization constitutes a data breach. This could include unauthorized access by employees, hackers, or other third parties.

Loss of Data: If personal data is lost, whether through accidental deletion, theft, or any other means, it is considered a data breach. This includes physical loss of devices containing personal data (e.g., lost or stolen laptops, USB drives) as well as loss due to technical failures or errors.

Destruction of Data: Intentional or unintentional destruction of personal data without proper authorization constitutes a data breach. This could occur through deliberate actions (e.g., deleting data to cover up a security incident) or accidental deletion due to system errors or malfunctions.

Alteration of Data: Any unauthorized alteration or manipulation of personal data constitutes a data breach. This includes changing, tampering with, or falsifying personal data in a way that affects its accuracy, integrity, or reliability.

Disclosure of Data: If personal data is disclosed to unauthorized parties, whether intentionally or accidentally, it constitutes a data breach. This could occur through external breaches (e.g., hacking, phishing attacks) or internal breaches (e.g., unauthorized sharing of data by employees).