Data Protection Policy

Date:	Review Period*:	Reviewed by:	Authorised by*:	Next Review Date:
Sept 2022	2022/2023	Chris Enoh	Geoffrey Opoku	Sept 2023
Sept 2023	2023/2024	Geoffrey Opoku	Chris Enoh	Sept 2024
July 2024	2024/2025	Chris Enoh	Geoffrey Opoku	July 2025

Approval Period: Annually*

* Unless there are changes in the law or circumstances in which case the policy and/or documents shall be revised accordingly

Approval Level Required: Governing Body or individual Governor

Document Version: V001/072022

Linked Policies: **n/a**

Appendices: **n/a**

Supreme Education
1433a London Road
London
SW16 4AQ
www.supremeeducation.org

Contents

Purpose:

This Policy is aimed at ensuring that Supreme Education implements rigorous and robust data protection measures. It sets out Supreme Education's systems, processes and expectations in relation to managing and maintaining protected data in compliance and accordance with applicable legislative and regulatory requirements.

Supreme Education will have mechanisms in place to protect the use and processing of protected data, as required, and processes for any required reporting of breaches.

Scope:

- This policy shall apply to all Staff members who will access and/or process data, including protected data, of which Supreme Education is in possession in order to carry out the functions typically associated with teaching facilities such as Supreme Education.

Policy:

- Supreme Education shall endeavour to fulfill its legal obligations in relation to protected data.
- Supreme Education shall, during the natural course of the school's activities, be required to collect, store, and process personal data (including sensitive information) about Staff members, students, their parents, contractors, and other third parties.
- Supreme Education shall, for the purposes of data protection, be the "data controller" and liable for the actions of its Staff members and governors in how data is handled within Supreme Education.
- Supreme Education shall expect all Staff members to play their part in ensuring that the school remains in compliance with and mindful of its legal obligations as such relates to handling personal data. UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data. Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

1. Definitions

- The following definitions have been included for ease of reference and shall apply to the content of this policy, as appropriate and as the content and context dictates:
  - **Data Controller:** A person or body that determines the purpose and means in which personal data is processed, and who is legally responsible for how such is used, e.g., Supreme Education, including the governing body, shall be Data Controllers. Any independent

contractor/s linked to Supreme Education shall be responsible for effectively managing the protection of data, as required, and shall be their own data controller;

- **Data Processor:** An organisation that processes personal data on behalf of a data controller, e.g., an IT provider, payroll provider, or any other such supplier of appropriate outsourced services with whom personal data may be shared for the purposes of carrying out specific services but who is not authorised to make any decisions about how it is used;
- **Personal Data:** Personal information which relates to a living individual (a data subject) by which that individual may be personally identified i.e., an identifier, either digital or contextual, including names, unique ID numbers, initials, job titles, nicknames, etc. Supreme Education shall, as a normal part of carrying out business, be required to manage personal data.
- **Personal Data Breach:** A breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;
- **Processing:** This includes anything done with Personal Data, including (but not necessarily limited to) obtaining, collecting, structuring, analysing, storing, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering, deleting, etc.;
- **Special Categories of Personal Data:** Special categories relate to Personal Data that informs racial or ethnic origin, trade union membership, political opinions, religious or philosophical beliefs, medical and health conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual.

2. Policy Statement

- It is in everyone's interests to get data protection right and to handle all Personal Data fairly, lawfully, securely and responsibly.
- Any Staff member who has access to Personal Data, for whatever reason, should consider the following:
  - Would I be satisfied if my Personal Data is Processed in this way?
  - Can I stand by how I have Processed the Personal Data in an email or official record?
  - What would be the consequences of my losing or misdirecting this Personal Data?

3. Roles and Responsibilities for Data Protection at Supreme Education

3.1 Board of Governors

- The Board of Governors shall have overall responsibility for all matters relating to Data Protection within Supreme Education.
- The Board of Governors shall be responsible for appointing a governor who shall be the school's designated Data Protection Lead on behalf of the Board and Supreme Education.
- The Board of Governors shall regularly liaise with the designated Data Protection Lead regarding Data Protection risk assessments that shall be carried out on a regular basis.

3.2 Designated Data Protection Lead

- The designated Data Protection Lead shall be responsible for ensuring that all Personal Data for which Supreme Education is processed in accordance with the provisions contained in this policy and the principles of the UK General Data Protection Regulation (UK GDPR).
- The designated Data Protection Lead shall be responsible for carrying out regular risk assessments and reporting back to the Board of Governors with any concerns and recommendations.
- The designated Data Protection Lead shall be responsible for reviewing the applicable legislation quarterly and facilitate any policy updates, as required and appropriate.
- The designated Data Protection Lead shall be responsible for assessing and facilitating Staff training, including orientation training for new Staff members and ongoing refresher training for existing Staff members.

3.3 All Staff members of Supreme Education

- All Staff members are responsible for data protection within the school and shall adhere to the provisions of this policy.
- Any Staff member who have any questions and/or concerns about the operation of this policy and/or Data Protection and/or any concerns that the policy has not been followed should immediately seek advice, in the first instance, from the Data Protection Lead.
- All Staff members shall have headline responsibilities in relation to Data Protection including, but not necessarily limited to:

3.3.1 Record-keeping:

- Personal Data held by Supreme Education should be accurate, fair and adequate. Staff members should inform the designated Data Protection Lead of any Personal Data believed to be inaccurate or untrue. This also applies to the way in which Staff members record their own data, and the Personal Data of others;
- Staff members shall Process Personal Data in a professional and appropriate way.
- Staff members shall be made aware of the rights of individuals in relation to the Personal Data held on them, i.e. any individuals about whom the school records information on school business (including emails and notes), either digitally or in hard copy files, may have the right to see such information. Staff members should not be discouraged from recording necessary records of incidents, conversations, evaluations, etc involving colleagues or students, in accordance with the school's other policies. It should be understood that there may be grounds whereby such information must be withheld these.
- Staff members should ensure that they record, as required, in a form they would be prepared to stand by should the individual about whom it was recorded asks to see it.

3.3.2 Data Handling

- All Staff members shall have a responsibility to handle the Personal Data with which they come into contact with fairly, lawfully, responsibly, securely, and in accordance with all relevant school policies and procedures

3.3.3 Avoiding, Mitigating and Reporting Data Breaches

- If any Staff member becomes aware of any breach of Personal Data, such Staff member shall immediately notify the designated Data Protection Lead. Supreme Education is legally obliged to report certain breaches to the relevant agency (i.e., ICO).
- A breach of Personal Data may be serious or minor; and it may involve fault or not; however, Staff members have a duty to always inform the designated Data Protection Lead who will consult with the Board of Governors for a reporting decision.
- Supreme Education will not necessarily treat a Personal Data breach as a disciplinary matter – each breach shall be evaluated on merit; however, any failure to report a breach or alleged breached shall be deemed a disciplinary matter as it may result in significant exposure for the school, and for those affected.

4. The Principles of Data Protection

- It is the intention of Supreme Education to incorporate best-practise policy regarding data protection to ensure the appropriate levels of protection in relation to personal data that is Processed by the school.
- Supreme Education acknowledges and shall adhere to the 6 (six) principles of data protection, as contained in the UK GDPR relating to the Processing of Personal Data which states that Personal Data must be:
  - Processed lawfully, fairly and in a transparent manner;
  - Collected for specific and explicit purposes and only for the purposes for which it was collected;
  - Relevant and limited to what is necessary for the purpose it is Processed;
  - Accurate and kept up to date;
  - Kept for no longer than is necessary for the purposes for which it is Processed; and
  - Processed in a manner that ensures appropriate security of the Personal Data.
- Supreme Education shall Process Personal Data in a fair and legal manner which shall include, but not necessarily be limited to:
  - Managing and maintaining records of the school's data processing activities, e.g. through comprehensive logs and robust school policies and procedures;
  - Documenting risk assessments and significant decisions on the Processing of Personal Data;
  - Regularly reviewing the applicable legislation and best practice requirements to ensure that this policy is up-to-date; and

- Maintaining an audit trail of the school's data protection, privacy, confidentiality, and compliance endeavours, e.g., when policies are updated, Staff training, maintaining appropriate Data Protection consents collected from individuals, and how the school handles data breaches.

5. Lawful Grounds for Data Processing

- Supreme Education shall comply with the provisions of the UK GDPR with regards to the Processing of Personal Data in relation to the business operation of the school.
- Supreme Education may Process Personal Data, as permitted under the UK GDPR, on the following lawful grounds:
  - Consent;
  - Legitimate interest;
  - Compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
  - Contractual necessity, e.g. to perform a contract with Staff member, parents, contractors, etc.;
  - Grounds for Processing special categories of Personal Data which shall include explicit consent, emergencies, and specific public interest grounds.

6. Rights of Individuals

- The individuals who own the Personal Data being processed have certain specific rights over such Personal Data, including access to their Personal Data, i.e., subject access right.
- The individual may request access to the Personal Data the school has on them subject access request). Supreme Education shall deal with such requests promptly and the school shall require no formality for the request.
- Should a Staff member become aware of a subject access request (or any communication from an individual about their Personal Data), such Staff member shall inform the designated Data Protection Lead immediately.
- The individual may have the following legal rights that are unqualified and exceptions may apply:
  - Require Supreme Education correct the Personal Data held about them if such information is inaccurate;
  - Request that their Personal Data, subject to the requirements of the UK GDPR;
  - Request that Supreme Education restrict its data Processing activities in respect of their Personal Data (in certain circumstances);
  - Receive a copy of the Personal Data held by Supreme Education for the purpose of transmitting it in a commonly used format to another data controller, as applicable and appropriate;
  - Object to the Processing of their Personal Data, on grounds relating to their particular situation, should the individual feel that the processing has a disproportionate impact on them.
- The individual also has a number of absolute rights that must be adhered to, e.g.:

- The individual may object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- The individual may object to direct marketing; and
- The individual may withdraw their consent for processing their Personal Data (without affecting the lawfulness of Processing that was carried out prior to the withdrawal of the individual's consent.

 All request received from an individual regarding the Processing of their Personal Data shall be forwarded to the designated Data Protection Lead as soon as possible.

7. Data Security Measures

 Supreme Education shall implement appropriate security measures to be activated upon any unlawful or unauthorised processing of Personal Data, or accidental loss of, or damage to, Personal Data.

 These measures shall include, but are not necessarily limited to:

- All physical records containing Personal Data shall be stored in secure storage cabinets that can only be accessed by authorised Staff members;
- All Staff members are required to exercise due diligence to promote that electronic forms of the Personal Data remain secure at all times;
- Staff members whose job function requires them to access digital versions of Personal Data in computer systems will be given a unique role-based authentication password which will log their access to the system. A new password will be generated at least once every 90 (ninety) days.
- Any Staff member (both professional and support) who leave the employ of Supreme Education will have their access to the computer systems immediately terminated.
- Any Personal Data that is transmitted electronically may only be transferred across Supreme Education's secure and encrypted secure line. The security of transmission lines is verified in a contract with the third-party service provider responsible for the transmission of protected data.
- Digitally stored Personal Data may not leave the premises of Supreme Education without being encrypted first. This shall include laptops, mobile devices, flash drive devices and/or email transmission.
- Only Staff members with a business need to know are allowed to view, read or discuss any part of an individual's Personal Data.
- New Staff members will receive training and are required to familiarise themselves with the content of this policy, and annual training will be provided to all Staff members regarding the protection of Personal Data. This annual training will serve to remind Staff members that any viewing, reading or discussion around Personal Data, other than for business purposes, is strictly forbidden.
- Risk Assessments will be carried out annually by the designated Data Protection Lead and two additional appointed Staff members.

- Additional risk assessments will be carried out when:
  - New software/hardware is installed;
  - A new procedure is initiated;
  - There's a change or addition to the layout of the premises;
  - There's a significant change to an existing procedure.
- The designated Data Protection Lead will review the ICO website, a minimum of 3 (three) times a year, for updates, amendments or changes to policies, procedures, and legislation around data protection and protecting Personal Data and promote that these are implemented and that Staff training is provided to advise of same.
- No Staff member is permitted to remove Personal Data from the school premises, in any form (e.g., paper, electronic, etc), without the prior consent of the designated Data Protection Lead;
- No Staff member shall provide or disclose any Personal Data to third parties, including a volunteer or contractor, unless there is a lawful reason to do so;
- Supreme Education does not permit Staff members to use personal email accounts or unencrypted personal devices for official school business.

- When Processing financial and/or credit card data, Staff members shall comply with the requirements of the PCI Data Security Standard (PCI DSS). Staff members undertaking such Processing may only do so if they are aware of and comply with the most up to date PCI DSS requirements. Any Staff member who is unsure in this regard must seek further guidance from the Head before Processing such data.
- When Processing Personal Data relating to criminal convictions and offences, Staff members shall do so in compliance with the prevailing legislation. Any Staff member who is unsure in this regard must seek further guidance from the Head before Processing such data.

8. Application of the Policy

- This policy establishes the standard of compliance expected within Supreme Education from those tasked with handling (in whatever form) and/or Processing Personal Data, including Staff members, contractors, third party agents, etc.
- Where Supreme Education shares Personal Data with third party data controllers, including (but not necessarily limited to other schools, parents, appropriate authorities, casual workers, and volunteers), each party shall be required to have a lawful basis to Process such Personal Data, and shall be expected to Process such Personal Data lawfully and with due regard to security and confidentiality, as set out in this policy.
- This policy sets out Supreme Education's expectations and procedures with respect to Processing any Personal Data within the school (including parents, pupils, employees, contractors and third parties).
- Staff members are required to comply fully with the provisions contained in this policy. Failure to comply with the provisions of this policy may result in disciplinary action being taken against such Staff member which shall be determined on a case -by-case basis.

- Staff members are required to report any alleged or suspected breaches of this policy as such a breach may pose significant risks to the school and/or individuals.

Procedure:

- All Staff members of Supreme Education shall follow the direction of the policy. Should any Staff member be in any doubt about how the policy informs the procedure, such Staff member must immediately seek advice from the Head Teacher.

9. Procedure Handling Images, Digital Images and Social Media Content:

Purpose

This section outlines the principles and procedures for the handling, storage, and dissemination of images, digital images, and social media content within Supreme Education. It aims to ensure the privacy and protection of students, staff, and other individuals while complying with relevant data protection laws and best practices.

Scope

This sub-policy applies to all staff, students, volunteers, and contractors of Supreme Education who have access to or manage images, digital images, and social media content. It covers all forms of image capture and distribution, including photographs, video recordings, and social media postings.

Key Principles

- **Consent and Permissions**
  - Prior written consent must be obtained from parents or guardians for capturing and using images of students.
  - Consent forms should clearly explain the purpose, usage, and duration of the image storage.
  - Staff and visitors must also provide consent for their images to be captured and used.
- **Usage and Distribution**
  - Images and videos should only be used for the purposes explicitly stated in the consent forms.
  - Distribution of images must be limited to authorized platforms and channels as per the consent agreements.
  - No images should be posted on personal social media accounts of staff or students.
- **Storage and Security**
  - Digital images must be stored securely with access restricted to authorized personnel only.
  - Images should be stored on Supreme Education-managed devices or secure cloud storage with appropriate encryption.
  - Physical copies of images should be stored in locked, secure locations.
- **Social Media Management**
  - Official Supreme Education social media accounts should be managed by designated staff members.
  - All content posted on official accounts must adhere to Supreme Education's content guidelines and privacy policies.
  - Any identifiable images of students posted on social media must have appropriate consent, and care should be taken to ensure students' identities and privacy are protected.

- **Retention and Deletion**
  - Images should be retained only for as long as necessary for their intended purpose.
  - Once the purpose has been fulfilled or consent has been withdrawn, images must be securely deleted or destroyed.
  - Regular audits should be conducted to ensure compliance with retention and deletion policies.
- **Monitoring and Compliance**
  - Supreme Education will regularly monitor the use and dissemination of images to ensure compliance with this policy.
  - Any breaches of this sub-policy must be reported immediately to the Data Protection Officer (DPO).
  - Disciplinary action may be taken against individuals who violate this policy.

- **Data Audit Process**

  - Supreme Education will conduct regular audits of all collected images and digital content to ensure compliance with data protection laws and internal policies.
  - The audit process will include checking for proper consent documentation, verifying the secure storage of images, and ensuring that images are being used for their intended purposes.
  - Audit findings will be documented, and any non-compliance issues will be addressed promptly with corrective actions.

- **Data Minimisation**

- Supreme Education will adhere to the principle of data minimisation by ensuring that only the minimum amount of personal data necessary for the specified lawful purpose is collected and processed.
- Consent forms and data collection processes will be designed to gather only essential information.
- Regular reviews will be conducted to evaluate the necessity of the collected data, and unnecessary data will be deleted or anonymised.

Responsibilities

- **Data Protection Officer (DPO):** Oversee the implementation of this sub-policy, conduct training, and ensure compliance with data protection regulations.
- **Staff:** Obtain proper consent, handle images responsibly, and report any concerns or breaches.
- **Students and Parents:** Understand and adhere to the terms of consent provided for image use.

Training and Awareness

- Regular training sessions will be conducted to educate staff and students about the importance of data protection concerning images and social media.
- Information about this sub-policy will be communicated clearly to all stakeholders at the beginning of each academic year and upon any significant changes.

By adhering to this sub-policy, Supreme Education ensures the responsible and lawful management of images, digital images, and social media content, safeguarding the privacy and rights of all individuals involved.