RHK Education

Data Protection Policy

Last review: August 2025

Approved: R Knight

Contents:

Statement of intent

1. Legal framework (updated)
2. Applicable data
3. Accountability
4. Data protection officer (DPO) (updated)
5. Lawful processing
6. Consent
7. The right to be informed
8. The right of access
9. The right to rectification
10. The right to erasure
11. The right to restrict processing
12. The right to data portability
13. The right to object
14. Automated decision making and profiling (updated)
15. Data protection by design and default
16. Data Protection Impact Assessments (DPIAs) (updated)
17. Data breaches
18. Data security
19. Safeguarding
20. Publication of information
21. CCTV and photography
22. Cloud computing (updated)
23. Use of generative artificial intelligence (AI) (New)
24. Data retention
25. DBS data
26. Monitoring and review

Statement of intent

RHK Education is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

RHK Education may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, DfE, referring schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how RHK Education complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and RHK Education believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE (2024) 'Keeping Children Safe in Education 2024'

This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2023) 'Data protection in schools'
- DfE (2025) 'Generative artificial intelligence (AI) in education'

This policy operates in conjunction with the following RHK Education policies:

- Electronic Devices Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Records Management Policy

2. Applicable data

For the purpose of this policy, **'personal data'** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

3. Accountability

RHK Education will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

RHK Education will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

RHK Education will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

Alternative Education Providers are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise RHK Education and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor RHK Education's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with RHK Education's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout RHK Education community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.
- Providing annual training for all staff on the risks, limitations, and lawful processing requirements when using generative artificial intelligence (AI) technologies.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to education. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at RHK Education, which is the governing board.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

The DPO at RHK Education is Ruth Knight

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked RHK Education to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by RHK Education in the performance of its tasks

RHK Education will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.

- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

RHK Education has privacy notices for the following groups, which outline the information above that is specific to them:

- Pupils and their families
- Employees
- Volunteers

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where RHK Education relies on:

- 'Performance of contract' to process a child's data, RHK Education considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, RHK Education takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, RHK Education ensures that the requirements outlined in the 'Consent' section are met, and RHK Education does not exploit any imbalance of power in the relationship between RHK Education and the child.

6. Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

RHK Education ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join RHK Education, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where RHK Education opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, RHK Education obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by RHK Education on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how RHK Education uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time
    - Lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that RHK Education holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

8. The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. RHK Education will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, RHK Education may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a SAR has been made for information held about a child, RHK Education will evaluate whether the child is capable of fully understanding their rights. If RHK Education determines the child can understand their rights, it will respond directly to the child.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, RHK Education holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

RHK Education will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, RHK Education will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

In the event that a large quantity of information is being processed about an individual, RHK Education will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

9. The right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, RHK Education may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. RHK Education reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

RHK Education will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. RHK Education will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, RHK Education will inform them of the rectification where possible. Where appropriate, RHK Education will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, RHK Education will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

10. The right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

RHK Education will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

RHK Education has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

RHK Education has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, RHK Education may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, RHK Education will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including children, have the right to block or suppress RHK Education's processing of personal data.

RHK Education will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until RHK Education has verified the accuracy of the data
- Where an individual has objected to the processing and RHK Education is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where RHK Education no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, RHK Education will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. RHK Education will inform individuals when a restriction on processing has been lifted.

Where RHK Education is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, RHK Education will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

RHK Education reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12. The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. RHK Education will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

RHK Education will provide the information free of charge.

In the event that the personal data concerns more than one individual, RHK Education will consider whether providing the information would prejudice the rights of any other individual.

RHK Education will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, RHK Education will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to object

RHK Education will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately

from any other information. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- RHK Education will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where RHK Education can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- RHK Education will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and RHK Education will stop processing personal data for direct marketing purposes as soon as an objection is received.
- RHK Education cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- RHK Education will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, RHK Education is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, RHK Education will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. RHK Education will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, RHK Education will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. Automated decision making and profiling

RHK Education will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- RHK Education has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

RHK Education will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

RHK Education will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

RHK Education will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, RHK Education will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15. Data protection by design and default

RHK Education will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how RHK Education has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, RHK Education will ensure that only data that is necessary to achieve its specific purpose will be processed.

RHK Education will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in RHK Education ICT systems.
- Implementing basic technical measures within RHK Education network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

16. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with RHK Education's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

DPIAs will allow RHK Education to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to RHK Education's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

RHK Education will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, RHK Education will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17. Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at RHK Education, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Where RHK Education faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of RHK Education becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, RHK Education will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

RHK Education will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

RHK Education will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

18. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Where digital data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, RHK Education enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Where possible, staff will not use their personal laptops or computers for RHK Education purposes. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

If staff need to use their personal laptops for RHK Education purposes, particularly if they are working from home, they will bring their device into RHK Education before using it for work to ensure the appropriate software can be downloaded and information encrypted.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.

Before sharing data, all staff will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from RHK Education premises accepts full responsibility for the security of the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of RHK Education containing sensitive information are supervised at all times.

The physical security of RHK Education's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

RHK Education will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

RHK Education takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The head of centre is responsible for continuity and recovery measures are in place to ensure the security of protected data.

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

RHK Education holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

19. Safeguarding

RHK Education understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

RHK Education will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The director will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.

- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

RHK Education will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

RHK Education will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. RHK Education will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, RHK Education will seek independent legal advice.

20. Publication of information

RHK Education will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to RHK Education website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

RHK Education understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

RHK Education notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for six months for security purposes; the head of centre is responsible for keeping the records secure and allowing access, where the footage is then subject to a disciplinary processes, safeguarding procedures or criminal investigations it will be shared in line with legal compliance and kept until no longer required.

RHK Education also has body worn cameras which are used as part of our CCTV monitoring and used for collecting images, videos and sound during specific incidents and when staff are accompanying pupils to the local shops. RHK Education notifies all pupils, staff and visitors including parents of the purposes of collecting images from body warn cameras and that they do not intrude on privacy and are necessary to fulfil their purpose. All body worn footage will be kept for six months for security purposes, the head of centre is responsible for keeping the records secure and allowing access, where the footage is then subject to a disciplinary processes, safeguarding procedures or criminal investigations it will be shared in line with legal compliance and kept until no longer required.

Before RHK Education is able to obtain the data of pupils or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

RHK Education will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. If RHK Education wishes to use images or video footage of pupils in a publication, such as RHK Education website, prospectus, or recordings of RHK Education plays, written permission will be sought for the particular usage from the parent of the pupil. Precautions, as outlined in the Photography Policy, are taken when publishing photographs of pupils, in print, video or on RHK Education website.

Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

Parents and others attending RHK Education events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to RHK Education.

RHK Education asks that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

22. Cloud computing

For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves RHK Education accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, the school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the school to audit or verify compliance where necessary. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a RHK Education device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on RHK Education devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert RHK Education should unauthorised access, deletion or modification occur, and ensure ongoing compliance with RHK Education's policies for the use of cloud computing.

RHK Education's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with RHK Education's Data Protection Policy.

- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should RHK Education decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether RHK Education is prepared to accept that risk.
- Monitor the use of RHK Education's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

23. Use of generative artificial intelligence (AI)

RHK Education recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in provision operations.

Use of generative AI tools must comply with RHK Education's Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the DPO and will be investigated in line with RHK Education's data breach procedures.

24. Data retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of RHK Education may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

25. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

26. Monitoring and review

This policy is reviewed by the DPO and the quality consultant. The next scheduled review date for this policy is August 2026.