KINGFISHER
EDUCATION GROUP

DATA PROTECTION POLICY - STAFF

Responsible:	Director
Date Reviewed:	January 2025
Review Period:	Annually
Approval Authority:	Governors
External Release:	Yes

General Statement of Duties

Kingfisher Education takes the privacy and security of your data seriously. We gather and use information or 'data' about you as part of our business and to manage our relationship with you. We will comply with the legal obligations under the Data Protection Act 2018 (DPA 2018) and the EU General Data Protection Regulation ('GDPR') which sits alongside the UK GDPR (with effect on 1st

January 2021) in respect of data privacy and security. Our duty is to notify you of the information contained in this policy.

This policy applies to all of Kingfisher Education employees whether current, past or prospective, as well as their parents and guardians. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy.

Kingfisher Education is the 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of processing of your personal data.

This policy outlines how Kingfisher Education will collect and manage your information. It details your right as the 'data subject', including the rights of parents as well as those of our students aged 12 years and older to access their personal data.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.'

It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to

come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, doctor or reference contact/agency) or it could be created by us.

We may collect and use the following types of personal data about you (but is not limited to):

- Your names, contact details and date of birth;
- Emergency contact details;
- Your recruitment information such as your application form, CV or similar.
- Bank details;
- Your student passport details in case you require an invitation letter for visa reason;
- Name of any friend(s) student wishes to share a room with / request to be in the same class or specialist option group with
- Information relating to disciplinary proceedings involving you (whether or not you were the main subject of those proceedings);
- Attendance records;
- Progress reports and examination results;
- Your images (whether captured on CCTV, by photograph or video) if relevant; and
- Any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data

Special categories of personal data' are types of personal data consisting of information as to:

- Your racial or ethnic origin;
- Your religious or philosophical beliefs;
- Your genetic or biometric data;
- Your health;
- Your criminal records and proceedings

It is unlikely that we will require such data, except for health-related information. However, in specific circumstances, we may need to retain and utilise any of these special categories of personal data in compliance with legal requirements.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage;
- Adaptation or alteration;
- Retrieval, consultation or use;
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination; and
- Restriction, destruction or erasure.

This includes the handling of personal data that is part of a filing system, as well as any automated processing involved.

How will we process your personal data?

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the DPA 2018.

We will use your personal data for:

• Implementing your employment contract between us
• Complying with any legal obligation; or
• If it is necessary for our legitimate interests (or for the legitimate interests of someone else).

However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

We may handle your personal data for purposes without your awareness or consent. If we plan to use your personal data for different purposes, we will inform you and clarify the legal requirements.

If you choose not to provide us with certain personal data that we require, you should be aware that we may not be able to pay you. It may also prevent us from complying with legal obligations such as paying the correct amount of tax set by HMRC.

We process your personal data in various ways during your recruitment and employment and even following termination of your employment.

For example:

- When we decide whether to employ you;
- Implementing your pay grade, and the other terms of your contract with us;
- To confirm that you have the legal right to work for us;
- To carry out the contract between us including where relevant, its termination;
- Training and performance review*;
- For promotion considerations;
- To manage your performance, absence or conduct;
- To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- To determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- To monitor diversity and equal opportunities;
- To monitor and protect the security (including network security) of the Company, of you, our other staff and students
- To monitor and protect the health and safety of you, our other staff, students and third parties;
- To pay you and provide pension and other benefits in accordance with your employment contract;
- Paying tax and national insurance;
- To provide a reference upon request from another employer;
- Monitoring compliance by you, us and others with our policies and our contractual obligations;
- To comply with employment law, immigration law, health and safety law, tax law and other laws where appropriate;
- To answer questions from insurers in respect of any insurance policies that may relate to you;
- Running the business and planning for the future;
- Prevention and detection of fraud or other criminal offences;
- To defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- For any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for

your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying out rights and obligations;
- Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- Where you have made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is required for the purpose of occupational medicine of for assessing your working capacity.

We may process special categories of personal data for the purposes above in particular, we will use information in relation to:

- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits.
- To comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

Sharing your personal data

At times, we may share your personal information with affiliated companies or our contractors and agents to fulfil our contractual obligations to you or to pursue our legitimate interests.

We require these companies to maintain the confidentiality and security of your personal data, ensuring it is protected in line with the law and our policies. They are authorised to process your data solely for the legitimate purpose for which it was shared and in accordance with our directives.

It maybe that we decide to outsource our payroll services or accounts at some point and we will need to share personal data for these purposes.

We might also need to share your data with professional organizations and affiliated entities, such as the British Council and the British Activity Providers Association. These organisations assess our courses to ensure we adhere to established quality standards.

We do not transfer your personal data beyond the European Economic Area. Should this policy change, you will be informed and provided with details about the measures in place to ensure the security of your data.

How should you process personal data for the Company?

- Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.
- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work.

This includes telling us if your own contact details change.

- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- It maybe that we will ask that personal data is either encrypted or put in a password protected document if it is transferred internally or externally.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the person responsible for Data Protection.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager.
- Personal data should be shredded and disposed of securely when you have finished with it.

- You should ask for help from the person responsible for Data Protection, if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

How to deal with data breaches

We have implemented measures to reduce the likelihood of data breaches and to prevent them from occurring. In the event that a personal data breach happens—whether it affects you or someone else—we are required to document and maintain evidence of the incident. If the breach poses a potential risk to the rights and freedoms of individuals, we are also obligated to inform the Information Commissioner's Office within 72 hours.

Subject access requests

- Individuals have the right to submit a 'subject access request' ('SAR') to discover what information we possess about them. This request must be submitted in writing. If you receive such a request, please forward it promptly to your line manager, who will manage the response.
- We are required to reply within one month, unless the request is complex or involves multiple items. In such cases, the response time may be extended by an additional two months.
- There is no cost associated with submitting a SAR. However, if your request is clearly unreasonable or overly burdensome, we may impose a reasonable administrative fee or decline to respond to your request.

It is important to be aware that some data is excluded from the right of access under the Data Protection Act. This includes information that identifies other individuals, data that we reasonably believe could cause harm or distress, and information protected by legal professional privilege.

EEA/EU Representative

Now that the UK has left the EU, we are required as per Article 27 of Regulation (EU) 2016/679 (General Data Protection Regulation - "the GDPR") to appoint an EU Representative as a point of contact for EU citizens to get in touch with us about their data.

Gallery Teachers, a division of Roxinford Education Group Ltd, is hereby appointed as EU Representative to Exsportise Limited. Gallery Teachers has offices in the UK, Italy and Spain.

The following tasks are the responsibility of the Representative:

- Help Kingfisher Education provide individuals with access to their data subject rights
- Act as the main point of contact for Supervisory Authorities
- Alert Kingfisher Education to any correspondence received from Supervisory Authorities
- Alert Kingfisher Education to any inquiries received from data subjects
- Be readily available to carry out the above mentioned work

All notices, demands, or requests should be sent to: admin@kingfishereducation.com

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.
- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do you should contact the person responsible for Data Protection or your line manager.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.

In general, we will not depend on your consent as a legal basis for processing your data. However, if we do seek your consent for a specific purpose related to the processing of your personal data, you have the right to refuse or withdraw that consent at any time. To withdraw your consent, please reach out to your line manager.

You have the right to raise a complaint with the Information Commissioner. You can accomplish this by reaching out directly to the Information Commissioner's Office. For complete contact details, including a helpline number, please visit the Information Commissioner's Office website (www.ico.org.uk). This site also provides additional information regarding your rights and our responsibilities.

Unsuccessful Employee Applications:

If your application is not successful, all documents associated with it will be securely destroyed within 12 months from the date you are notified of the outcome, unless retention is required for legal or regulatory purposes.