Employees - Data Protection Policy 2024

General Statement of Duties

The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (DPA 2018) and the EU General Data Protection Regulation ('GDPR') which sits alongside and supplements the UK GDPR (with effect on 1st January 2021) in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former employees, workers, volunteers, apprentices, and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue you from time to time concerning your data.

The Company is a '**data controller**' for the purposes of your data. This means that we determine the purpose and means of processing your personal data.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data while working for, or on behalf of, the Company.

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 with other materials.

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

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- your contact details and date of birth.
- the contact details for your emergency contacts.
- your gender.
- information about your contract of employment (or services), including start and end dates of employment, role and location, working hours, details of the promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement.
- your bank details and information in relation to your tax status, including your national insurance number.
- your identification documents, including your passport and driving licence and information in relation to your immigration status and right to work for us.
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).
- information relating to your performance and behaviour at work.
- training records.
- electronic information in relation to your use of IT systems/swipe cards/telephone systems.
- 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 such as:

- your racial or ethnic origin.
- your political opinions.
- your religious or philosophical beliefs.
- your trade union membership (if relevant).
- your genetic or biometric data.
- your health.
- any criminal convictions and offences.

It is unlikely we will need to hold such data apart from data regarding your health. However, in certain situations, we may need to hold and use any of these special categories of your data in accordance with the law.

How we define processing

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

- collection, recording, organisation, structuring, or storage.
- adaption or alteration.
- retrieval, consultation, or use.
- disclosure by transmission, dissemination, or otherwise making available.

- alignment or combination; and
- restriction, destruction, or erasure.

This includes processing personal data, which forms part of a filing system, and any automated processing.

How will we process your personal data?

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

We will use your personal data for the following:

- performing the contract of employment (or services) 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 can process your personal data for these purposes without your knowledge or consent. We won't use your personal data for an unrelated purpose without telling you about it and the legal basis we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following the termination of your employment (or engagement).

For example:

- to decide whether to employ (or engage) you.
- to decide how much to pay you, and the other terms of your contract with us.
- to check you have the legal right to work for us.
- to carry out the contract between us including where relevant, its termination.
- training you and reviewing your performance.
- to decide whether to promote you.
- to decide whether and how 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, customers, and others.
- to monitor and protect the health and safety of you, our other staff, customers and third parties.
- to pay you and provide pension and other benefits in accordance with the contract between us.
- 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 which affect us.
- to answer questions from insurers in respect of any insurance policies which relate to you.
- running our business and planning for the future.
- the 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 under employment law.
- 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 necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your 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

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

It may be 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 may also need to share your data with professional organisations and affiliated bodies, such as the British Council and The British Activity Providers Association, which inspect our courses to ensure we meet agreed quality standards.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

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 may be 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 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 the 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 measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

Subject access requests

- Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to your line manager who will coordinate a response.
- We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.
- There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.
- Please note that certain data is exempt from the right of access under the Data Protection Act, such as information which identifies other individuals, information which we reasonably believe is likely to cause damage or distress, or information which is subject to 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 British Summer School. Gallery Teachers has offices in the UK, Italy and Spain.

The following tasks are the responsibility of the Representative:

- Help British Summer School. provide individuals with access to their data subject rights
- Act as the main point of contact for Supervisory Authorities
- Alert British Summer School. to any correspondence received from Supervisory Authorities
- Alert British Summer School. 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: dpo@galleryteachers.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 most situations, we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact your line manager.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Unsuccessful Employee Applications:

If your application is unsuccessful, all documentation relating to your application will be confidentially destroyed no later than 12 months after the date you are informed of the outcome, unless it is necessary for legal or regulatory compliance.

Signed:

Danny Kenward
Operations Manager, British Summer School

Date: 1 November 2023
Review Date: 1 October 2024