Data Protection Policy

September 2025

Aim and scope of this policy

This policy applies to the processing of personal data in manual and electronic records kept by the Company in connection with its human resources function as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Company makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees' conduct themselves in line with this, and other related, policies.

Where third parties process data on behalf of the Company, boomsatsuma Education Limited will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data. In line with current data protection legislation, the Company understands that it will be accountable for the processing, management and

regulation, and storage and retention of all personal data held in the form of manual records and on computers.

This Policy does not form part of your contract of employment

Types of data held

Personal data is kept in HR files or within the Company's HR systems. The following types of data may be held by the Company, as appropriate, on relevant individuals:

• Name, address, phone numbers - for individual and next of kin
• Application forms, CVs and other information gathered during recruitment •
References from former employers
• National Insurance numbers
• Job title, job descriptions and pay grades
• Conduct issues such as letters of concern, disciplinary proceedings •
Holiday records
• Internal performance information
• Medical or health information including reasonable adjustments required •
Sickness absence records
• Tax codes
• Images of you from our on-site CCTV systems
• Terms and conditions of employment
• Training details.

Special category data and data relating to criminal convictions or offences

Special category data is information as to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; your health; details of your sex life or sexual orientation.

We may collect information from you relating to some of these matters but will usually do so in an anonymised way so as to monitor the effectiveness of our Diversity, Equality and Inclusion policy. Where this is the case it will not be considered to be personal data. However, where the data has not been anonymised or pseudonymised, this will clearly be special category data and be treated as such.

Details of any special category data the Company may collect and process about you will be explained in detail to you when the data is collected from you.

The Company processes personal data relating to criminal convictions to meet our legal obligations and to meet regulatory requirements including Safer Recruitment obligations.

Where data is held

The Company holds personal data about you within:

● our intranet
● security records and systems

● time keeping records
● telephone recording or monitoring systems
● CCTV
● email systems
● electronic and paper HR files.

Relevant individuals should refer to the appropriate Company's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the Company will:

• be processed fairly, lawfully and in a transparent manner;
• be collected for specific, explicit, and legitimate purposes;
• be adequate, relevant and limited to what is necessary for the purposes of processing;
• be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay;
• not be kept for longer than is necessary for its given purpose; and • be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisational measures.

Lawful processing

In line with the data protection principles we will only process your personal data and special category data for the reasons notified to you and in accordance with our obligations. Under the DRA we must have a specified lawful basis for processing your personal data.

The Company processes personal data where necessary to manage the employment relationship and the main lawful bases for processing your data are:

• to comply with our legal obligations (e.g. paying your tax),
• to perform your contract with us (e.g. pay you according to the rate agreed), and • because it is necessary for our legitimate interests (e.g. to ensure that we can succession plan).

Where one of these reasons applies we may process your data without your consent. You may choose not to give us certain data but you should be aware that this may prevent us complying with our legal obligations and this may in turn affect your employment.

Where we process special category data we will only do so where one of the lawful reasons set out above applies and where either: you have given your explicit consent; processing is necessary under employment law; processing is necessary to protect your or another person's vital interests and you are incapable of giving consent; you have made the data public; processing is necessary to do with a legal claim; it is necessary for occupational medical reasons, or for the assessment of your working capacity. Where we plan to process special category data relating to you we will explain this, and set out the reasons, at the time.

Your rights as a "data subject"

All relevant individuals:

• have the right to be told what personal data the Company processes, how this processing takes place and on what basis.
• have the right to see your own personal data by making a subject access request (see below).
• have the right to receive a copy of your personal data and in some circumstances have your personal data transferred to another data controller, usually within a month, and without any charge.
• can correct any inaccuracies in your personal data by contacting the HR administrator;
• may ask the Company to erase personal data where it is no longer necessary to process it for the purpose it was collected or where it should not have been collected in the first place.
• may object to data processing where the Company is relying on a legitimate interest to do so and you think your rights and interests outweigh ours.
• will be notified if there is a data security breach involving your data that may affect you.
• have the right not to consent, or to later withdraw your consent to processing where we were relying on consent as the lawful reason to process personal data. • have the right to complain to the Information Commissioner. Contact details can be found on their website: www.ico.org.uk.

Requests for access to this data will be dealt with under the following summary guidelines:

• The request should be made to Joe Sallis, IT Manager;
• the Company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request;
• the Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Company will take immediate steps to rectify the information.

Subject access requests

All employees have the right to review the information that the Company holds about them, with some exceptions. If you wish to make a 'subject access request' you should write to the Company's Data Protection Officer/HR.

The Company will usually respond within one month. If your request is complex the timescale for a response may be extended by up to two months. Where this is the case, we will advise you of this within one month of receiving your request and explain why we need more time

No charge will usually be made for a response to a subject access request.

If you receive a subject access request from another employee you should immediately forward it to the IT Manager or the HR adviser.

Data security

The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data security policy.

In addition, employees must:

• ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
• ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
• refrain from sending emails containing sensitive work related information to their personal email address
• check regularly on the accuracy of data being entered into computers • always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
• use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the IT Manager. Where personal data is recorded on any such device it should be protected by:

• ensuring that data is recorded on such devices only where absolutely necessary • using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
• ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers

The Company does not transfer personal data to any recipients outside of the EEA.

Data security and your obligations

Access to employee data will be restricted to those users with a specific and legitimate business need for the data. If you have access to personal data pertaining to other employees or clients/customers etc. then you must familiarise yourself with this policy, including the data protection principles and comply with them.
All employees have obligations in regard to handling data at work. Specifically:
• you must keep your own personal data up to date. The Company will prompt you to review it from time to time but any changes between such reviews should be notified to us as soon as practicable.
• you must keep all data secure - whether on paper or electronically. Use strong passwords and always lock your PC/device when you are not using it. Keep personal data in locked cabinets.
• you must only access data which you are authorised to, and then you must only process that data for the reasons set out in this policy and in line with the data protection principles.
• you must securely destroy any copies of personal data you create. • you must not share personal data with anyone not authorised to see that personal data and should consider at all times whether there is a way to share data that might disclose less information, e.g. anonymising data or redacting documents where necessary.
• personal data must not be stored on your own personal devices and printed copies should not be removed from Company premises unless you have specific authorisation for this.

• do not share personal data with sources external to the Company unless authorised to do so, and only when the data has been encrypted or otherwise made secure. • do not transfer personal data outside the European Economic Area unless this has been authorised in advance by the Company's IT Manager.
• if you receive a subject access request, immediately refer it to the IT Manager. • if you become aware of a possible data security breach, however minor, immediately report it to the IT Manager.

If you are ever in any doubt as to your obligations please contact the Company's IT Manager, who is responsible for Data protection matters, for clarification.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller for the Company will be trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Breaches of this policy

An employee found to be in breach of this policy will be liable to disciplinary action up to and including, in cases of serious or deliberate breach, summary dismissal for gross misconduct.

Monitoring

The Company has the right to monitor your use of the Company's computer systems (including your emails and use of the internet on workplace computers or other devices) because it needs to do so to protect other employees and because of duties owed to suppliers and clients.

If any other monitoring is being considered you will be advised of this and given all the relevant information, including the lawful basis for processing the data, at the time such monitoring is put in place. In all cases a Privacy Impact Assessment will be undertaken.
Covert monitoring will only take place exceptionally and where the Privacy Impact Assessment has established that there is no less intrusive way to gather the information.

Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

Data protection compliance

Joe Sallis is the Company's appointed compliance officer in respect of its data protection activities.

Approval

Approved by; Beth Griffiths

Date; September 2025

Role;

Review date; September 2026

boomsatsuma Education Ltd