

Data Protection Policy

Policy statement from Square Bell Ltd



This policy is effective from 01 November 2023 until and unless it is superseded by a newer version.

General

Square Bell provides data processing services to education organisations, such as data transfer and validation services, and analyses for performance management or monitoring purposes. In providing these services, the school or other originating organisation remains the data controller at all times.

Square Bell complies with all relevant UK and EU data protection regulations and with the UK Information Commissioner's Office (ICO) mandate. Where appropriate, Square Bell will also assist data controllers to comply with their own obligations.

Terms of service

The general terms and commitments outlined in this document apply to all Square Bell services and operations. Additional details may be provided for specific services or added to your contract if appropriate. A separate privacy policy also applies to personal data controlled by Square Bell.

Our Use of Data

The Use of Data policy is provided for source organisations such as schools to ensure that, as data controllers, they can share data and that they consider there to be appropriate measures in place, ensuring that the data is held securely and confidentially. This document sets out how Square Bell supports these objectives.

Square Bell and its suppliers will be acting as a data processor under UK data protection law. Square Bell has taken all reasonable measures to ensure the safety and security of personal information and continues to review these measures on an on-going basis. Square Bell are registered with the Information Commissioner's Office (ICO) with registration number ZA154335.

When you take up a service from Square Bell, we will provide you with a document that outlines the specific details of the data processing involved for that service. This will include details of the data items processed, the nature of the processing, and the recipients of any outputs or onward transfer of the data. We will only process your data in line with the specifications for the service, unless required by law to act otherwise.

Data will only be collected as it is required and will be destroyed upon termination of the agreement with the client. The source organisation that originates the data (e.g. school/university) remains the Data Controller. Data controllers have the right to terminate their agreement with Square Bell at any point and personal data held by Square Bell will be destroyed within 10 working days of termination.

Where our service is providing information to a third party such as a Local Authority or Multi-Academy Trust, the data collected will be reported to the third party either in aggregate or individual detail, as appropriate. Once communicated to end users, Square Bell is not responsible for the security or use of the information held by the third party.

Data Security

This information gives details of the management of data security in relation to the use of Square Bell. You may wish to use this in conjunction with your fair use policy.

Information may be extracted automatically from a school or other organisation's Management Information System (MIS) using a secure method by one of our data partners, with whom you will have a separate data sharing agreement. The data is then securely transferred to Square Bell using industry standard encryption. A unique identifier configured by Square Bell ensures that the information is linked to the correct customer account.

If we need to arrange a non-automated transfer of data from you to Square Bell, we will provide suitably secure mechanisms for the transfer. For example, via upload or data entry direct to our websites, or by using a secure email solution.

The information from your organisation is held inside the Square Bell systems. Our systems all require a unique user's security credentials (such as username and password) for access. We use security measures such as full disk encryption and field-level encryption of personal data where appropriate.

Data on portable systems such as laptops and memory sticks will always be stored encrypted to reduce risk. Data transferred electronically will use transport layer security (e.g. SSL) where available, and file- or message-level encryption as appropriate. We will never transfer or transport personal data via insecure methods.

Transfer of data outside the UK

Square Bell will not transfer personal data to any country, territory, or organisation that does not provide adequate protection for individuals' rights and freedoms for their personal data. We follow the UK adequacy regulations relevant to the GDPR.

Your data may be processed in other countries in the European Economic Area, unless a separate undertaking to keep data in the UK is included in our contract or other agreement.

Third party sub-processing

We use the third-party organisations listed below to provide content-neutral administrative and infrastructure functions with which we deliver our services. These providers are all committed to ensuring data is adequately protected under UK law and only retain or process data in provision of the functions below to Square Bell, except where they also have a separate agreement with you as the data controller.

Provider	Functions provided to Square Bell
Groupcall	Data extraction and transfer from school MIS
Wonde	Data extraction and transfer from school MIS
Krystal Hosting Ltd	Virtual Private Server for web hosting and email
Amazon Web Services	Secure data storage, provision of secure computing environments, user authentication, and web hosting
Microsoft (Azure and Online Services)	Secure data storage, provision of secure computing environments, user authentication, and web hosting

Support

The Support team at Square Bell are able to resolve or advise you on any technical issues that you encounter while using our products, and also provide first line support for data partner integration. Occasionally it can be necessary for our support technicians to view the issue with you, in order to diagnose it fully and offer a solution. In circumstances where support technicians need to view the issue, they may use remote access tools to view your computer with you, in which case you should remain at your computer and supervise the entire session.

All of our remote sessions allow you to retain control and allow you to terminate the session at any time. If your issue escalates and an additional support technician is required, then they may also be invited to join the remote session. In some cases where a second line escalation is required for our data partner software this may involve also allowing a data partner support technician to join the remote session.

If your issue is a platform issue or requires changes to your account configuration, then Square Bell staff may perform such configuration on your behalf from our secure management platform without requirement for remote access. You are reminded that you should avoid sending personal information, such as student/contact records, to us directly via email. You certainly should only send such information when supported by strong encryption, if there is an explicit requirement to do so. Square Bell staff will advise the most secure method for transfer if there is such an explicit requirement.

Data Life Cycle

Your data's point of origin remains your organisation's own system (e.g. school MIS). For services where data is collected via automated means, changes made in the MIS are transmitted to Square Bell through one of our data partners on a regular synchronisation schedule.

A copy of your data is held and maintained by Square Bell while this agreement is in place and while the data is needed for ongoing processing, analysis, and production of reports. Information will be provided on an agreed schedule to you, or to your Local Authority, Multi-Academy Trust or other partner, as appropriate. Our service-specific documentation will specify all the recipients of data who may make ongoing use of your information. We will not share your data with any organisations other than those identified unless we are compelled to do so by law.

Once Square Bell's contracted work ends or after you terminate your agreement with us, the data collected from you will be deleted from Square Bell's systems. If we have provided information to a third party as part of the service, such as your Local Authority or Multi-Academy Trust, they may still retain copies of any data or reports provided to them.

Data Controllers' responsibilities

As the originating organisation, you remain the data controller for any data you have provided to Square Bell and retain responsibility for the rights of your data subjects. This includes informing the data subjects of the way their data will be processed.

Square Bell will assist you in enabling data subjects to exercise their rights over data held by Square Bell, but we do not provide systems to validate, approve, or action requests direct from data subjects unless explicitly agreed with you in a separate contract.

Square Bell will also assist the data controller in meeting data protection obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.

About this policy

Who to contact if you have queries about this policy

If you have any questions about the details of Square Bell's services or systems please contact Chris Mullarkey at chris.mullarkey@squarebell.com or call on 0115 7141234.

If you have a query or concern relating to our data protection practices, please email dataprotection@squarebell.com

Updates to this policy

We may update this policy from time to time and we will send advance notification to your main account contact if this is the case. All our policies will be regularly reviewed in preparation for, or following enactment of, new UK data protection regulations and other relevant changes.

Document version history

This section is not part of the Square Bell Data Protection Policy.

Version 1.5

Update to list of sub-processors, adding Wonde and removing Assembly, Dropbox, and Egress.

Update “Transfer of data outside the UK” section, removing reference to EU-US Privacy Shield, restricting to EEA, and including clarification that data can be retained within UK if specifically required.

Version 1.4

Update to list of sub-processors, including removal of LGfL and Digital Ocean.

Version 1.3

Added section on transfer of data outside the UK.

Update to list of sub-processors, including addition of Dropbox and Digital Ocean.

Minor changes to wording.

Added this Version History section and changed version numbering format.

Version 0.2.1 effective from 2018-05-25 onwards

Prepared to reflect changes required for compliance with the GDPR. Superseded the older “Terms of Service” document.