Arbor

GDPR
At Arbor
How We Comply

One of the key principles GDPR puts into law is **'privacy by design'**, meaning that security features should not be pasted on top of any system, but should be an integral part of how that system is constructed. When you buy from Arbor, that's exactly what you're getting.
Whether you're a headteacher, a MAT leader, or a Data Protection Officer, these answers should address any concerns you have about using our products from May 25th, 2018 and beyond.

Contents

How does Arbor protect school data?

Arbor meets and exceeds the requirements of GDPR, protecting the data we store with a comprehensive Information Security Management System which the International Organisation for Standardisation (ISO) audits annually. This system is governed by our Information Security Management Committee, which consists of senior management across various business areas.

You can download our **updated Terms and Conditions**, and read more about data protection at Arbor, **here**.

Physical security procedures

Physical security is maintained by formal security inspections, risk assessments and access control at every Arbor office. Access to Arbor locations is restricted with secure keys, CCTV, 24/7 security personnel and secure perimeter doors.

Digital security procedures

Data security is maintained not only by our staff's awareness training and personal vigilance, but by a number of digital safeguards. Staff passwords are changed regularly and wherever possible all our business systems require two-factor authentication. Data is kept on our central system rather than any individual device, making it easy to give and revoke permissions to different users.

What security certificates do you have?

- The international benchmark for data security is the ISO 27001 standard. Arbor maintains ISO 27001:2013 certification. Certificate number LRQA 10015370
- Our server infrastructure provider, Amazon Web Services, is also certified with ISO 27001, ISO 27017 and ISO 27018
- Arbor is certified with Cyber Essentials. Certificate number 0016298130002077
- Our ICO Data Protection Registration number is Z3022381
- We are on the DfE cloud supplier checklist, and the G-Cloud list of approved cloud suppliers

How do you store school data?

Arbor is fully cloud hosted in Amazon Web Services UK's London servers. All personal data is physically stored, processed and managed from the UK. Backups are also stored in the UK.

All our architecture is housed in a private firewalled network to reduce external access and increase security. We operate a strict single-tenanted database model - this means that data is segregated from other customers in our database and persistence layers. Instances are recycled daily to reduce the risk of data being compromised, and all servers are patched continuously to reduce security vulnerabilities. Encryption in transit is through bank grade 256-bit SSL.

Our Insight dashboard and reports are also processed in these servers and equally compliant.

Is the rest of your supply chain secure?

Arbor maintains back-to-back contracts with our subcontractors so that all data security policies and responsibilities flow down to them, meaning all school data is kept secure. These standards are renewed every year, keeping protection up-to-date.

Our server infrastructure is maintained by engineers who work at Arbor Education Partners d.o.o., which is a fully-owned subsidiary company of Arbor Education Partners Group Ltd. They are subject to the same GDPR compliant security procedures as our central staff, plus our server security requirements. Access to servers by our engineers requires individual SSH keys, registered in an LDAP server, which are additionally password protected.

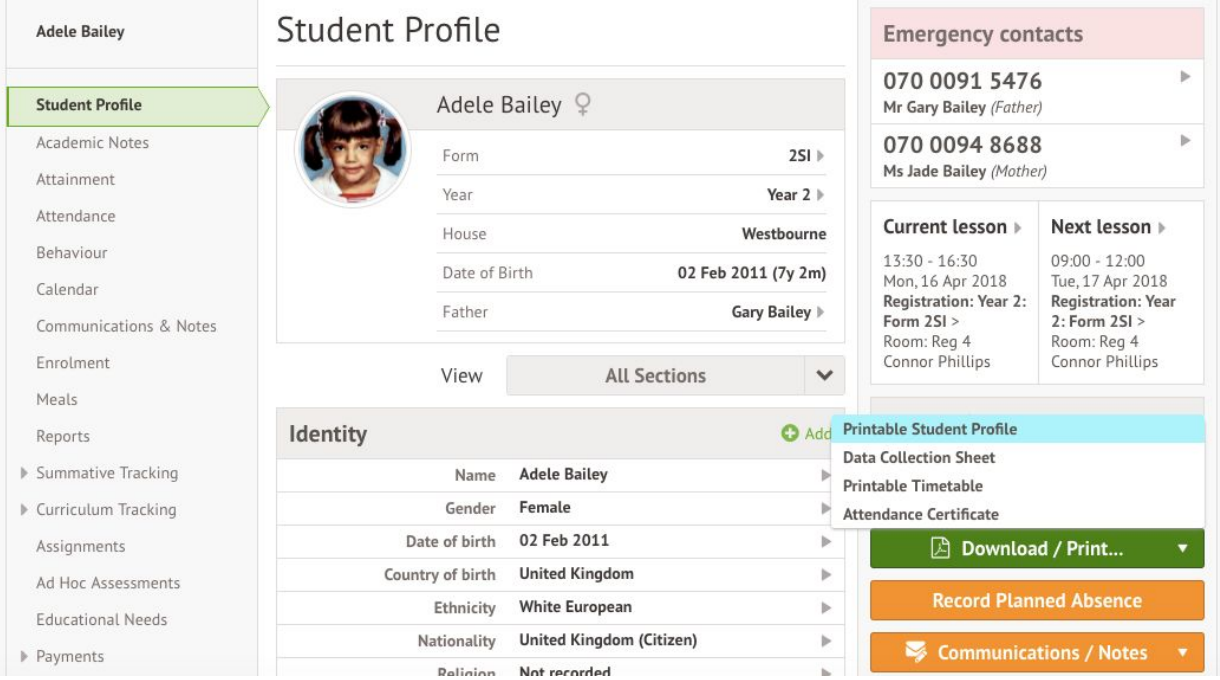
What's your policy for third-party apps?

Arbor can replace a lot of the third-party applications used by schools alongside their legacy MIS, but we welcome integration from your other processors with our open RESTful API. Once we've vetted your apps for compliance, they can become an Arbor approved partner. We can migrate your app data from your previous MIS to sync with Arbor. Nobody will be able to access your Arbor-stored data without the explicit, written consent of the data controller in your school.

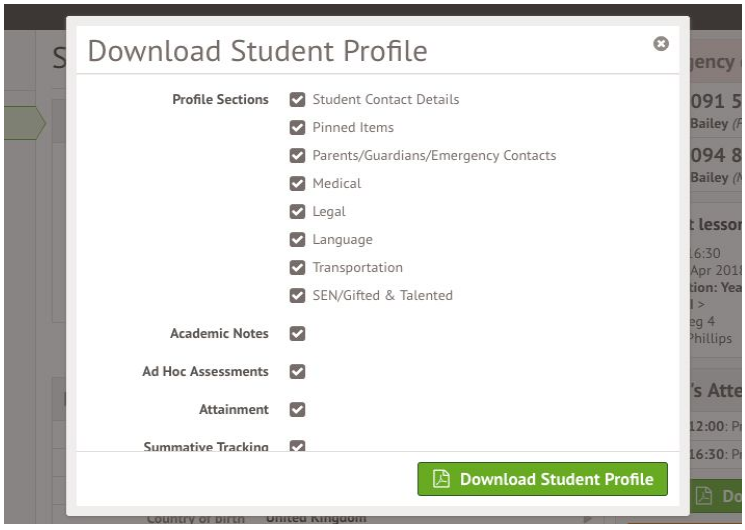
You can find a list of third-party organisations which have already been approved here. You'll be able to grant or reject access from the partners you use, and revoke their access at any time. All our partners have to prove their own GDPR compliance, and in particular a fine-grained permissions model that only gives data access to those who need it.

Is it easy to comply with GDPR's 'Subject Access Requests'?

Arbor will make every reasonable effort to help you get what you need from our system, and this includes helping you comply with Subject Access Requests in a secure way. Unlike some legacy MIS systems which hold different types of data in a variety of separate places throughout your school, Arbor can show you all the information you have permission to access about a student or staff member directly from their profile page.

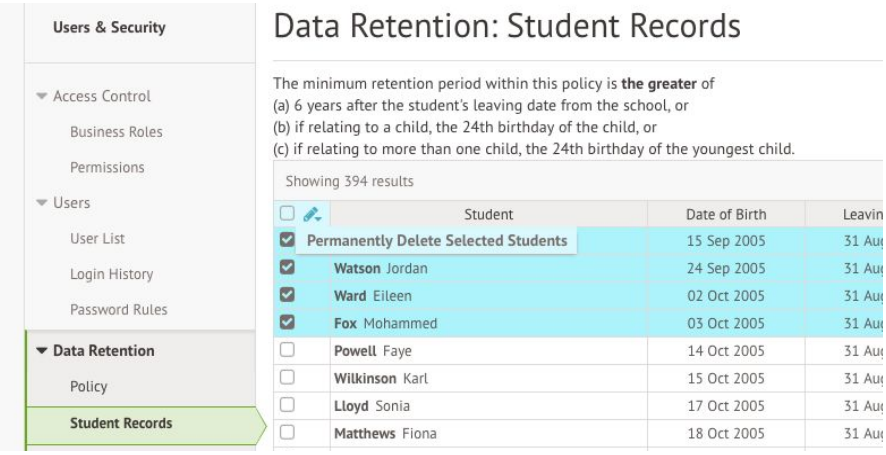


If you are a school or MAT leader, your role will enable you to retrieve all the personal data held about that subject on Arbor in a few clicks.



How can data be deleted from Arbor?

It's simple for schools to comply with their GDPR responsibility to delete unnecessary data, using our built in Student and Staff Data Retention dashboard. You can sort profiles by different categories and delete whole groups in moments - this means you could easily find and remove all the students who left your school more than six years ago!



Arbor will be able to restore the system to any point in the past 30 days in the case of accidentally deleted data. If you wish to terminate your Arbor contract, we can export your data to a new MIS using our open RESTful API, or directly to you in a standard CTF or CSV file format, and all your data will be deleted from our servers within 30 days as per our Data Retention Policy*.

As our Insight dashboards and reports are based on ASP data rather than data entered by the user, there is no personal information to delete. Arbor receives secure, early access to ASP data via a tender with the Department for Education. You can stop using your Insight account at any time. The latest, up-to-date ASP data will still be analysed for you if you decide to log back in.

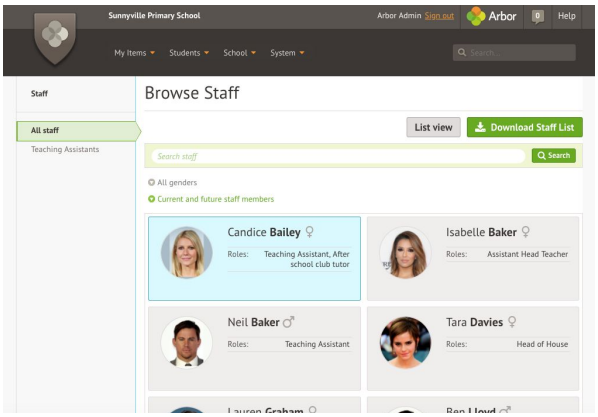
Will you be able to restore systems in an emergency?

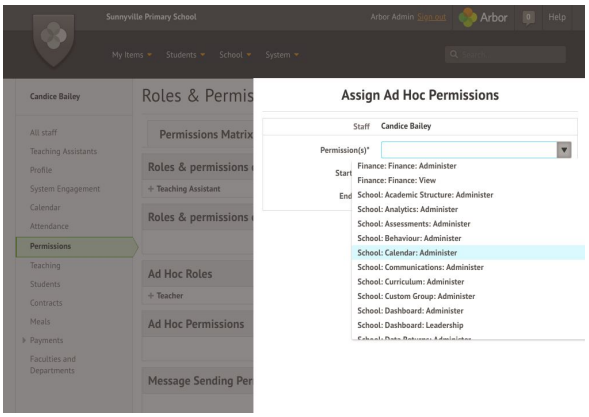
Arbor maintains a full Business Continuity Plan* which is regularly reviewed by our Information Security Management Committee, and each business unit has its own continuity plan tailored to the local conditions of that office. In the case of physical disruption, our cloud-based systems allow for rapid relocation to minimise disruption.

Our Devops team maintain a continuity plan in the case of server loss. All server configuration is stored as code, and we are able to establish an entire new set of server infrastructure within 24 hours. Snapshot backups are taken daily and also point-in-time backups are maintained, which means we can restore the system to any point in the last 30 days. Our backup restore procedure and the rest of these policies are regularly tested and audited.

How can school users control access to Arbor MIS?

One of the most powerful ways Arbor protects your school data is permission based access. Each user has a level of permission planned in collaboration with you when Arbor is implemented, that ensures they can only view the data relevant to their role. This is useful because GDPR demands you only let people access data that's necessary for their job, and only for as long as necessary.





You might give your pastoral team the ability to view and edit child protection data, whilst a child's form tutor can only view it, and a teacher who never works with them cannot access it at all. These role based permissions are built into every Arbor feature and can be given and taken away by the school on an ad hoc basis, giving you the flexibility you need to comply with GDPR without interrupting your flow of work.

How is data kept up to date and accurate?

Because Arbor is based on live data, entered in real time by the school, it is always as complete and correct as the school wishes it to be. You'll be able to review and search the data of students and staff on our easy to use dashboards and profile pages, and edit it whenever necessary, which will change the data across the entire system instantly. You can keep your old policies about how often you update personal data, and divide up the responsibility by giving administer permissions to different users.

The school or MAT leader will have access to a dashboard that also shows when each user has logged into the system, including Arbor's own admins. We can provide you a full audit of the actions of each of these users on your system on request.

We update Insight dashboards & reports as soon as possible after we receive the latest, most up-to-date ASP data from the Department for Education. This means your dashboards and reports should always show the latest, most accurate data.

How else does Arbor MIS help keep schools secure?

Each user has a secure and unique password, and we support a number of additional security features, including password rules, enforced regular password changes, and two-factor authentication by SMS or a physical Yubikey dongle. We plan all of this with the school when Arbor is implemented, and tailor MIS setup to your unique requirements.

In a cloud-based MIS like Arbor data isn't stored on any device, and Arbor automatically logs out after a period of inactivity. This means that even if there's a breach in your school's physical security, the data kept with us is less likely to be compromised. By accessing our cloud through their staff login, Parent Portal or Student Portal, users won't have to print or e-mail personal data, again reducing the risk it falls into the wrong hands.

Arbor's Access Control Policy

Our Access Control Policy* doesn't grant access to any systems unless there is a justified business need. Each system has a business owner, and a policy that governs who can gain access and what justifications support a user being granted privileged access.

Checking & Training Our Staff

All our staff and contractors undergo a DBS check, and employees require two references before starting work. All staff who need to access customer data receive data protection and information security awareness training as part of their induction, followed by our continuous professional training program. All staff involved in information security management have both significant industry experience, and formal training on the skills required.

Revoking Permission

When employees leave Arbor, their access to all business systems is revoked within 24 hours as part of our off-boarding procedure. We conduct semi-annual access control audits for every business system, and those users with business owner or administrator level permissions have their access reviewed quarterly.

The objective of our access policy, for both schools and our own staff, is that every user will have permission to access only the level of data that they need to do their job, and only for as long as they still need it. All these policies are also audited as part of our ISO 27001 certification.

Do you regularly assess your system's risks and vulnerabilities?

Yes. Our Devops team monitor for new vulnerabilities. Any new threats deemed a high risk are assessed by our engineering management, and a response plan is formulated.

All server operating systems are automatically patched with the latest security fixes every night. All software libraries are upgraded to the latest version, incorporating security fixes, upon every new release of our software (this happens at least once per day). An internal security committee assesses our software and infrastructure every month for possible vulnerabilities, and plans fixes for any they find. External penetration testing is also conducted annually.

How would you be alerted to a breach or error?

All servers are monitored for standard key metrics (CPU, memory, network load, requests). These metrics are collected into a central monitoring server, whilst all logs are collected into a centralised logging system. Alert trigger rules are defined on both metrics and logs to proactively alert our Devops team to possible issues and unusual activity. These alerts are investigated within several hours and resolved.

All errors within the application, including those reported by schools, are collected into a central error collection system. Each error is assigned to an engineer, who attempts to reproduce and, if necessary, fix the problem within 1 business day.

How would you respond to a data breach?

As soon as we became aware of a breach we would notify you without undue delay. Our established incident management process ensures we will gather all the evidence of the breach into a full incident report.

All incidents are detected and reported to our Chief Technical Officer, Emile Axelrad, who then is responsible for coordinating our technical teams, gathering evidence, assessing the incident, and managing the response plan. All communications procedures will be followed, the incident will be logged, and corrective action will be taken to mitigate the risk in the future. Our Security Incident Response Plan* is audited as part of our ISO 27001 certification.

* We can send any of these policies to Arbor users in full on request. If you have more questions about GDPR or Arbor in general, please get in touch!

Arbor

Interested in how Arbor can help?

www.arbor-education.com

hello@arbor-education.com

+44 (0) 207 043 0470

Canalot Studios 407

222 Kensal Road

London W10 5BN