BridgeU Data Protection - Frequently Asked Questions

Is BridgeU GDPR compliant?

Yes, we comply with the principles and requirements of the UK Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR). BridgeU takes its responsibilities to protect the security, confidentiality, integrity and privacy of your data very seriously, and continuously reviews and improves its technical and organisational approach to protecting data and privacy.

Where can I find BridgeU's statements on data protection?

You can find our privacy policy, that describes how we process personal data we collect from you or that you provide to us, here https://bridge-u.com/platform-privacy/. You can also find our policy on cookies, which are small text files that a website may put onto your device in order to help provide service to you, here https://bridge-u.com/cookies/. We will inform you when we make any changes to these policies.

Where is my data stored? Where are BridgeU servers located?

Our data is stored in the cloud. That means that the data lives on computers that are based in secure facilities in a number of countries around the world. We work with schools all around the world and using the cloud means that our website operates well wherever it is accessed from.

We only store personal data in, or transfer personal data for processing to, countries that are in the European Economic Area (EEA), or are international countries recognised by the EU as providing adequate protection of personal data, or, in certain cases and only for schools based in China, to China.

In particular, we make use of cloud hosting services for the purposes of storing and processing personal data in Ireland (Amazon Web Services, Heroku) and the USA (Google Cloud Platform, Amazon Web Services, Heroku).

BridgeU

How is my data protected? How secure are the servers you use?

Your data is protected by industry-standard processes at every layer.

Our servers are maintained by our cloud platform providers, ensuring that the infrastructure that the platform runs on – both the hardware and operating system – is kept up to date by a dedicated team. We use automated alerts to ensure that the software our servers run is kept up to date too, and prioritise security updates.

In addition to that, we take extra precautions to restrict access to data and ensure its integrity. Our databases use encryption-at-rest, meaning that even in the unlikely event of unauthorised access to the cloud servers, data is inaccessible.

Finally, any connections to BridgeU servers are secured by HTTPS and other encryption technologies, using the latest recommendations for encryption strength. This protects your data from any network-based attacks.

What level of encryption do you use across your site?

We currently generate our HTTPS certificates using LetsEncrypt and AWS Certificate Manager. Both of these currently secure connections with the following properties, but as our certificates are regularly rotated these may increase as and when industry recommendations change:

Connection to our servers are encrypted and authenticated using the TLS 1.2 protocol, an ECDHE_RSA with P-256 key exchange, and the AES_128_GCM cipher. Our key size is 2048-bit. These properties are all rated as “strong” by browsers.

How frequent are your site backups?

We perform full site backups at least daily, and additional ad-hoc backups depending on our development workflow.

The purpose of these backups is disaster recovery and are not designed for recovering from accidental user error. However in emergency situations we can attempt recovery from our backups on a best-effort basis.

How does BridgeU use student, staff and parent personal data?

We store and process personal data of students, staff and parents, when a school is considering to enter into an agreement with BridgeU, or when an agreement is in place and BridgeU is providing

the service to a school. The school is the data controller and BridgeU is acting as the processor of personal data on behalf of the school.

We process personal data in order to provide service, to analyse use of our website to better understand how people use our service, to make the website better, to administer the service, and to notify users about changes to the service.

We may send service, maintenance and other transactional emails to users of the website. Transactional emails are sent in response to a users using or administering the service, and include things such password reset emails, maintenance announcements, and changes to the service, features or supported browsers.

We may send non-transactional emails to users, such as newsletters, but only when either the user has explicitly opted to receive these emails, or where we believe, or have been informed, that the user has a legitimate interest in receiving targeted email communications. In either case, we make it easy for users to opt-out of receiving non-transactional emails.

What data does BridgeU collect?

As well as the data that users and schools provide about themselves or others on BridgeU, such as name and email address, we keep records of correspondence, information from our partners (e.g. ManageBac), device-specific information (e.g. the kind of device used to access BridgeU), network information (for administration and analytical purposes), and details of your visits to our website.

Can I opt out of sharing my data with BridgeU?

If a student, staff member, of parent objects to their data being processing by BridgeU on behalf of the school, we will not be able to provide the service to that individual.

Is any of my data shared with third parties?

We use a variety of carefully selected third parties to fulfil essential activities (e.g. processing data, storing data, and analysing data). We only use third parties that also comply with the GDPR. We only transfer personal data to a third party that stores data in the EEA, or in a country determined by the EU to provide adequate protection of personal data, or, in certain cases and only for schools based in China, to China.

Some of the main third party services that we may use are:

To provide platform functionality

- ManageBac (if a school has an existing account there)
- iSAMS (if a school has an existing account there)

- Parchment (if document sending is enabled and used)

As providers of cloud hosting services
- Google (Cloud Platform)
- Amazon (Web Services)
- Heroku

For customer success and operations
- Salesforce
- Zendesk
- Google (Drive)

To allow us to monitor and improve our service
- Google (Analytics)
- Segment
- Amplitude
- Sentry
- Papertrail

Do you comply with EU-US or Swiss-US Privacy Shield?

BridgeU does not have operating subsidiaries in the US and so does not need to register for programs such as these. We do, however, ensure that any third party is registered with the US Department of Commerce where it is appropriate.

Do you have a Data Protection Officer (DPO)?

The responsibility for governance and oversight of data protection, and overall information security, is predominantly with BridgeU's Chief Technology Officer (CTO), but is reviewed by the leadership team of the company at the highest levels. We have determined that we do not currently need to appoint a DPO and this decision will be reviewed at least annually by the company's senior leadership team.