Our Compliance - Data Security

Edukey fully complies with the current DPA, and holds Cyber Essentials Certification.

Edukey Education Ltd has standardised policies and procedures to manage and protect the data that we process on behalf of our clients. We have significant experience in the education sector, working with hundreds of UK primary and secondary schools. Our policies are driven by our inherent knowledge of schools, our Cyber Essentials certification and our existing data protection compliance through our ICO registration.

We have implemented a plan to achieve GDPR compliance:

- ✓ Our Leadership Team (CEO/CTO and Business Manager) are fully aware of the new GDPR regulations and the impact this is likely to have on both Edukey and our clients
- ✓ We have made all our staff aware of the new regulations through GDPR awareness sessions
- ✓ We have conducted an audit of all personal data we hold or process, including where it comes from
- ✓ We have reviewed the legal basis for all personal data processing to ensure we are compliant and to ensure that, if required, we have the appropriate consent in place
- ✓ We have reviewed and updated our policies and procedures to ensure that we comply with all the rights of individuals under GDPR including processes for secure data deletion, handling Subject Access Requests etc.
- ✓ We have data protection by design throughout our processes and we will continue with this policy. We are also conducting new Data Protection Impact Assessments across the company.

Does the organisation hold any related security certifications, e.g. ISO27001, Cyber Essentials.

Edukey Education Ltd hold Cyber Essentials Certification.

Google Cloud and Rackspace data centres are certified to the international standard for information security, ISO27001.

Is there an up-to-date security policy covering all components of the solution under consideration?

Access to all parts of the infrastructure is available to Edukey Education Ltd staff on a need to know basis and access is always revoked as soon as a member of staff no longer needs access or leaves the company.

Security-centred code reviews and testing is performed on all newly developed features.

Regular vulnerability scanning is performed using in-house and independent (supplied by Acunetix) automated vulnerability scanners.

Security related updates for all software used across the infrastructure is installed in a timely manner.

Dual factor authentication is enforced for all Edukey staff and for all services used in relation to the product.

Describe the appropriately strong identification, authentication and authorisation technology controls in place to ensure users only have permission to access services they are entitled to.

All access to applications take place over encrypted (SSL 256bit) connections. User passwords are encrypted using strong one way encryption.
User access is based on individual usernames and passwords.
User passwords must be a minimum of eight characters long and contain at least one number and one capital letter.
Users have eight log-in attempts before they are locked out.

Additional levels of security can be added such as locking access to the school IP address so that users need to be on site to gain access.

Edukey Education Ltd commits to restrict access to customer data only to those individuals who require such access to perform their job function.

Describe the audit mechanisms used to monitor and where necessary, alert on the information assets and services comprising the solution.

Edukey Education Ltd has email notifications for failed login attempts to any of their resources. Furthermore, the company automatically blocks users after a certain number of invalid login attempts within a time window.

Edukey Education Ltd uses error log monitoring software (Loggly) to alert the company to unusual activity and any errors that could potentially impact security of operations.

Is regular vulnerability scanning and annual pen testing undertaken? What are the associated remediation / 'fix' regimes and timescales?
Regular vulnerability scanning is undertaken with both home grown (for code based scanning) software and industry standard software (Acunetix, for penetration testing/vulnerability scanning).
Fixing all identified potential security issues is prioritised and normally takes place on the same day when an issue is identified.

What policies and procedures are in existence covering patch management, authorised software and anti-virus?
Edukey Education Ltd operate a security policy which ensures all PCs are automatically updated, only use authorised software relevant to job roles, and use up-to-date Norton anti-virus software. All code releases are checked by at least one person (during a code review) and tested before being released to production server.

Enumerate and describe operational procedures covering:
i) Change management
In the event of a change then relevant management staff assess the need, impact and time-frame to enact the change. Edukey Education Ltd have testing servers to ensure thorough and rigorous testing is conducted prior to release and no impact is made on the 'live product' by end users.
ii) System acceptance testing
Thorough end user acceptance testing is performed by in-house testing team and product specialists. These tests emulate real-world usage on behalf of clients / users.
iii) Backups
Edukey Education Ltd back-up nightly and retain the last fourteen back-ups. Backups are managed by data centres and are redundant. They are in the same physical location (London) but on completely different servers.
iv) Disaster Recovery
Restore process is managed by Edukey Education Ltd and within 24 hours.
v) Business continuity

Key staff have responsibilities to ensure critical business activities are prioritised and restored. Non-critical activities are suspended and essential resources are focused to support critical ones. These are recovered when all critical activities have been resumed.

Describe relevant process and procedure surrounding incident management provision.
In the first instance schools should contact their dedicated Edukey Education Ltd account administrator for any security issues, serious or minor. Issues should be reported to support@edukey.co.uk or via 01348 800 100. Serious issues to be reported to Duncan Wilson, Director (duncan@edukey.co.uk) and/or the Business Manager / COO (craig@edukey.co.uk).

Edukey Education Ltd are committed to offering a transparent service whereby any customer who feels that he/she is not being dealt with appropriately can speak directly to the Director and/or Business Manager if they wish to. Telephone, email and remote support is instantly available.

In the event of a serious incident, schools will have the full support of the company's technical team as a matter of priority until the issue is resolved.

Enumerate and describe personnel procedures addressing:
i) The vetting and referencing checking of employees and contractors.
All Edukey Education Ltd staff are DBS checked.
ii) Confidentiality agreements
When appointed to Edukey Education Ltd, all employees must agree to accept the following confidentiality clause:
'You will not, either during your employment or thereafter, use to the detriment or prejudice of the Employer or any of its customers or, except in the proper course of your duties, divulge to any person, firm or employer or otherwise make use of:
1. Any confidential information about the Employer, its business, accounts, finances, research projects, pricing policy, future business strategy, marketing strategies and plans, customer lists, discount rates and sales figures arrangements with suppliers, tenders, pitches, plans or strategies;
2. Any other information designated as confidential which may have come to your knowledge in the course of your employment.
This restriction will continue to apply after the termination of your employment without limitation in time but shall cease to apply to any information or knowledge that subsequently comes into the public domain, other than as a result of unauthorised disclosure by you.'
iii) Awareness training
Edukey Education Ltd staff complete a robust induction training programme. Refresher sessions are held every 2-3 months and important issues are highlighted to staff as they arise.
iv) Mobile working
Laptops are encrypted using Bitlocker. Impersonation requests received via email for on-site visits must be approved by Edukey Education Ltd management. Google Apps Device Policy in place.
An impersonation request is when a member of Edukey Education Ltd's team need to access a school's account for technical support. Before they can do so, Edukey Education Ltd management need to approve access. Access can be locked down to the school's IP address if required.
v) Leavers' process
Staff accounts are disabled immediately by Edukey Education Ltd.

Detail the relevant Physical Security process and procedure regarding:
i) Access control / internal barriers

Edukey Education Ltd. building is alarmed. All internal doors are lockable.

ii) Clear desk policy

No papers are left on desks. Confidential documents are shredded by staff.

iii) Screen savers

PCs are locked when staff are away from their desks.

iv) Secure storage / waste disposal

No sensitive data is stored on removable media. All printouts contained in waste are shredded.

l) Enumerate the Business Continuity management structure and describe its plans

All data is replicated running a RAID configuration with multiple redundant disks to ensure that Edukey Education Ltd has multiple copies in the event of the company suffering a major disaster.

Edukey Education Ltd uses a high capacity data centres (Google Cloud and Rackspace) and all aspects of service provision are continually monitored. The company maintains a substantial buffer zone to allow for data fluctuations and capacity can be increased with minimal notice.

m) How is the data protected in transit and at rest, e.g. email encryption, SFTP, https?

Edukey Education Ltd. encrypt data that customers provide that is transmitted over public and private networks with a minimum of 256bit SSL.

All data is encrypted at rest within the company's data centres with a AES256 block-based encryption.

Email traffic from Edukey Education Ltd to other cloud service providers is encrypted by default.

Login details are further encrypted using one way encryption.

Where is the information being retained?

Edukey Education Ltd's servers are hosted by Google Cloud (ClassCharts) and Rackspace in London, UK. The data centre is staffed by a team of highly trained, on-site engineers and security experts who work around the clock to ensure that the systems are secure and running strong.

Data centres have built in multiple layers of redundancy, at every level - including physical security, power, cooling and networks. These redundancies help make the data centre more resilient and reliable.

Physical security: Rackspace is restricted by biometric authentication, keycards and 24 x 7 x 365 surveillance. These ensure that only authorised engineers have access to routers, switches and servers.

Google Cloud data centres incorporate multiple layers of physical security protections. Access to these data centres is limited to only a very small fraction of Google employees. They use multiple physical security layers to protect our data centre floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.

Power: Rackspace's power systems deliver conditioned power while protecting against sags, surges, swells, spikes and electrical noise. Uninterruptible power supplies (UPS) provide instant failover for continuity during a power outage. On-site, always-fuelled diesel generators are prepared to pick up the load quickly during extended outages.

Cooling: N+2 redundant chiller configuration uses a combination of centrifugal chillers, cooling towers, chilled water loop pumps and condenser water loop pumps - with redundant water sources.

HVAC: Rackspace's precision Heating, Ventilation and Air Conditioning (HVAC) environment includes HEPA-equipped air handling units and contaminants. In the event of an HVAC system failure, there are redundant HVAC systems for immediate failover.

Network: the network includes includes four transit providers allowing Rackspace to shift traffic as needed. This configuration, co-developed with Cisco, guards against single points of failure at the shared network level.

How will access to this information be protected, e.g. passwords, permissions, etc.
All Edukey Education Ltd staff use strong passwords and the company operates a hierarchy of permissions relevant to job roles. Furthermore, all Edukey Education Ltd staff accounts are locked to the company's IP addresses and special authorisation needs to be granted by the management team to access accounts from any other IP address.

Edukey Education Ltd staff requiring access to assist with technical queries require authorisation from the management team. These access requests are received by email and ensure that only authorised staff are granted access from the company's recognised IP addresses.

How long will the information be retained for?
Edukey Education Ltd will retain data for the duration of the contract between the school and the company.

When will the information be deleted?
Edukey Education Ltd will delete all data 30 days after closing the school's account. The data will be completely eradicated fourteen days later from the company's backups.

If a school cancels their contract with Edukey Education Ltd then their account is set into 'Awaiting Deletion' state. Deletion then occurs automatically within 30 days. Data remains in encrypted backups until the 30-day cycle is complete. All deletion of data and deletion of backup files are logged.

Who is responsible for deleting the information?
Edukey Education Ltd's Systems Operation Manager, CTO, will be responsible for deleting the information when the account is closed.