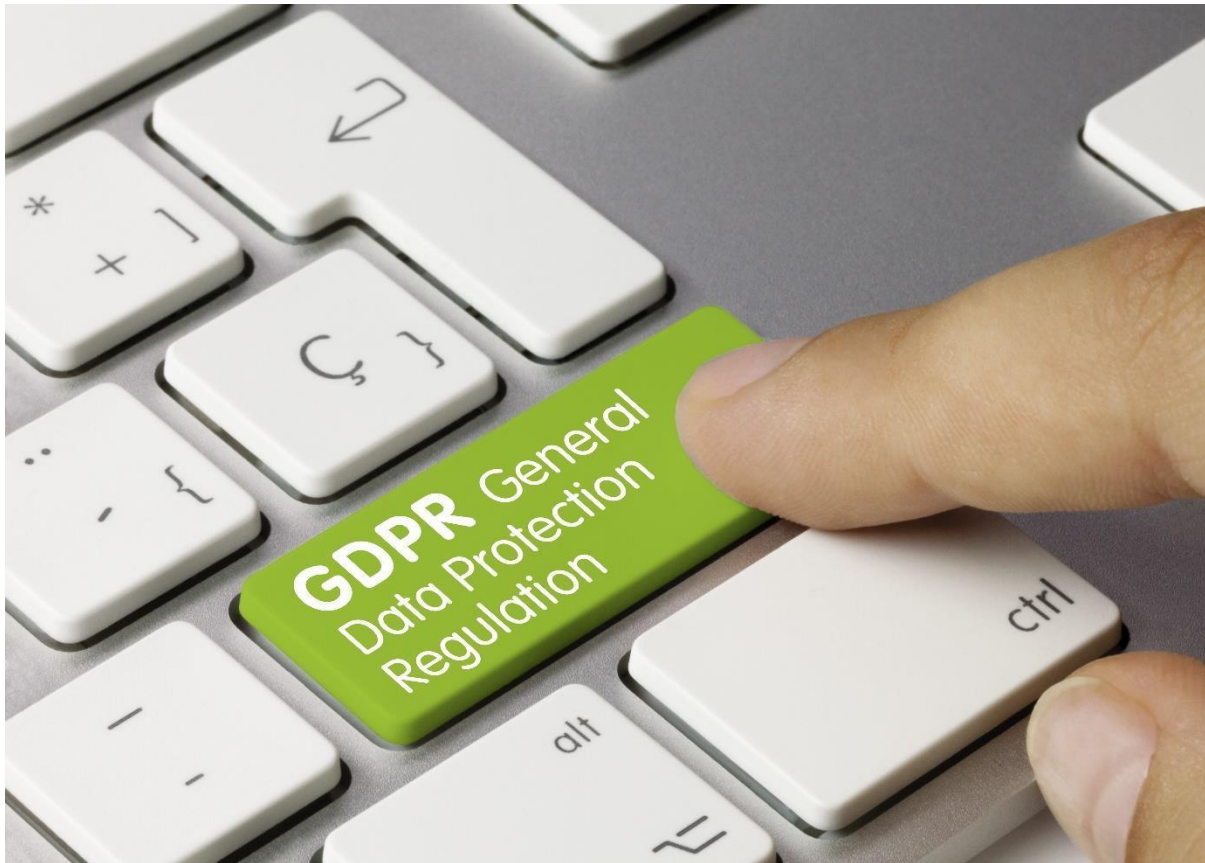


ContactGroup



GDPR Frequently Asked Questions from Schools

1. What action are you taking to prepare for the GDPR?

As a trusted processor of school data, we have had a GDPR readiness roadmap in place since the beginning of 2017. GDPR compliance is not an option for us and we are currently readying our business for compliance by the GDPR deadline on the 25th May 2018.

Our staff have been undergoing updated data privacy training to reflect the changing legislation. We have staff who have recognised accreditations EU General Data Protection Regulation Foundation (GDPR F) and EU General Data Protection Regulation Practitioner (GDPR P). We also have appointed a Data Protection Officer.

GDPR clearly outlines crucial changes to the data privacy rights of individuals, including the right to be forgotten, the right to move data from one platform to another (portability), the right to restrict data processing and the right not to be subject to automated profiling. Also important for educational establishments are data breach policies, which move to 72-hour reporting cycles.

The Contact Group have been refining internal procedures to help with this process, ensuring that all organisations in the data chain work together to provide the best service.

We are enhancing our product development to make sure that data protection by design is an integral part of the process. This includes considering DPIAs for any feature which impacts data privacy. We are also expanding our service to allow education establishments to contribute more to this process.

We are in the process of updating all of our privacy notices and data sharing agreements to reflect the GDPR changes. These include the data we process, our rationale for having it, and if we share it with any other organisation, the information that is shared and for what purpose.

This gives education establishments more visibility and control about what is happening to any data that they are authorising us to collect, and any information we collect via our services.

We are improving our services to enable schools to see what data we extract, when it was extracted, the consent flow and if we, or any third party used it.

Contact Group is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data in accordance with accepted standards including Cyber Essentials and ISO27001.

Contact Group will be fully compliant with applicable GDPR regulations when they take effect in 2018, including as a data processor, while also working closely with our customers and partners to meet contractual obligations for our procedures, products and services.

2. What technical and organisational security measures do you have in place to protect personal data?

All external connections to our systems are encrypted over SSL using and RSA 2048 bits DigiCert SHA2 Extended Validation certificate. All data held by Contact Group is encrypted both at rest and whilst in transit.

Contact Group undertakes regular internal and 3rd party security auditing of our applications and premises in order to ensure they adhere to customer expectations and current industry standards. Access to data by Contact Group staff is strictly controlled and audited.

3. What policies and procedures do you have in place to protect personal data?

Contact Group holds ICO registration to ensure continuing compliance with Data Protection legislation. All staff receive regular training regarding the latest best practices around data security. Contact Group has comprehensive DR policies and RTO's pertaining to the integrity and availability its services.

4. How secure are your systems?

All external connections to our systems are encrypted over SSL using and RSA 2048 bits DigiCert SHA2 Extended Validation certificate. All data held by Contact Group is encrypted whilst in transit.

5. Do you have any information management accreditation?

Contact Group holds ICO registration to ensure continuing compliance with Data Protection legislation

6. How is the data deleted and how often?

Customer data (for those who are no longer in contract with us) will be fully purged 30 days from the termination data of the contract unless specified otherwise. We don't hold data on anyone that is not in contract with us.

7. Do you hold the ISO 27000:2013 Information Security Management standard?

Although we are not currently ISO27001 compliant, we are in the documentation phase in direction for this.

8. Has Call Parents achieved any other form of security accreditation e.g. under the Government's Cyber Essentials scheme?

We have Cyber Essentials and our certificate number is 1639251624619545.

9. Where is your data hosted/stored?

The service sits either in-situ on school servers or on a hosted environment in a data centre in our Birmingham Head office building, UK. We do not rely on a third-party to extract data from schools. Our data extraction software requires minimal IT administration but if help is required a dedicated team of support staff are available to assist. Currently subject to data agreements we extract, Student, Staff, Parent, Telephones, Emails, Attendance, Behaviour and Timetable data for our products.

10. Are you GDPR compliant?

Contact Group is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data in accordance with accepted standards including Cyber Essentials and ISO27001.

Contact Group will be fully compliant with applicable GDPR regulations when they take effect in 2018, including as a data processor, whilst also working closely with our customers and partners to meet contractual obligations for our procedures, products and services.

11. Do you have a GDPR Statement?

Please click the link for our GDPR statement <https://www.the-contactgroup.com/gdpr/>

12. What country is the data held in?

In our personal data centre in Birmingham Head office building, UK.

Document uploads are stored on Amazon S3 (in Ireland – which are being moved to the UK before May-18).

13. Can an individuals' data be deleted from process?

This can be done manually at request from the school. We are looking to put processes in where this can be controlled by the School. But generally if the school does not want the data to be processed then they can

remove it from their MIS – and our next extract will remove it.

14. How long is data retained?

Generally, it is retained for as long as it is active in the MIS. If a school cancels or asks the data to be removed, it will be retained in our backup cycle for 30 days.

15. Why this timeframe?

We have automated backups for business continuity. The data in the backup itself cannot be accessed.

16. Can you please provide evidence that these are adhered to?

We are moving our processes to GDPR compliance for May.

17. Has Contact Group completed the DfE Cloud Services accreditation document?

Not currently, but we are currently working through this.

18. Has any independent penetration testing of their software taken place?

We have completed penetration tests for Call Parents and Looked After Call in April 2018 and are now in working on completing recommendations made.

19. Is the application protected by single factor authentication or two-factor authentication?

Single factor

20. Is data protected “in transit” AND “at rest”?

It is protected in transit. We are improving how are data is stored