G.D.P.R.

FAQ

Review Date: 11/12/2020
Next Review Date: December 2021
Signed: *Changing Education Group*

1. What is Cyber Essentials?

Cyber Essentials has been developed by UK Government and the National Cyber Security Centre (NCSC) to reduce the risk of organisations becoming victims of cybercrime. It is recommended by the Information Commissioners Office and provides an example of the technical measures that an organisation can take to comply with the UK Data Protection Act.

This annual assessment scheme requires us to ensure that we have implemented a series of technical measures, such as software patching, the use of complex passwords that help to protect Changing Education Group against the most common types of attacks. These measures should be taken by all organisations, regardless of size or sector.

As part of the annual assessment, the qualifying requirements are changed to reflect the evolving cyber threat as determined by the National Cyber Security Centre. This means that we are continuing to improve our cyber posture in line with the recommendations from experts.

More details about the scheme can be found at https://www.ncsc.gov.uk/cyberessentials/overview

2. What is IASME ?

The IASME scheme goes beyond the controls introduced with Cyber Essentials. This looks at the processes and procedures that are in place within the organisation and further strengthens our information security posture. Aligned to the international standard for information security (ISO27001), the scheme is further expanded to meet the fundamental requirements of the EU General Data Protection Regulation (EU GDPR) and the UK Data Protection Act 2018.

As part of our IASME assessment, which like Cyber Essentials is reviewed annually, we have reviewed and updated all of our procedures. These included procedures for Incident and Breach management, revisions of our Information Security & Data Privacy Policies, our training schedule with our staff and the Data Privacy policies that we share with our clients.

Developed by the same organisation who manage the Cyber Essentials scheme, the assessment criteria are reviewed on annual basis to ensure that the scheme continues to meet the requirements of business and was recently expanded to satisfy the requirements of the NHS Data Protection Toolkit and the NIS regulation.

Additional information on the IASME scheme can be found at https://iasme.co.uk/iasme-governance/

3. Isn't Cyber Essentials and IASME a self-assessment scheme? How do we know that you've not 'fudged' the answers?

Cyber Essentials and IASME are both self-assessment schemes and there's a common misconception that this is a 'tick box' process. We've engaged with an external specialist organisation called Risk Evolves to help us through the process. They have ensured that our business doesn't just meet but exceeds the requirement of the schemes.

To qualify, we have been required to submit responses to over 200 questions. Our responses are reviewed and assessed by an independent certification body prior to certification being issues. Each of the certification bodies are themselves assess by IASME to ensure that the level of accuracy is being maintained and that the integrity of the certification is upheld.

Finally, our Directors at Changing Education Group have to sign a declaration as part of this submission. Perhaps a sobering thought for anyone signing a declaration, if they were to sign knowing that they had 'fudged' any of the answers, they would be committing fraud.

4. What's a DPIA and why should I be interested?

A Data Protection Impact Assessment is a risk assessment and is a key mechanism to meet and demonstrate our accountability obligations under the EU GDPR and the UK DPA. It is a legal requirement to conduct a DPIA when processing certain types of data, where the loss, misuse etc could have a major impact on the 'rights and freedoms' of individuals. In a worst-case scenario, failure to undertake a DPIA could lead to an enforcement action or a fine from the ICO.

It is designed to ensure that the risks to personal data – whether this be loss, misuse etc are understood at the beginning of a project. Any risks identified should be managed and mitigated prior to the project commencing.

We have developed a DPIA for any data that we collect from Education Providers that can be used as input to their DPIA process. If you would like a copy then please contact our Data Officer, Stephen Hackney.

More information can be found on the Information Commissioners website : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

5. Where is data stored ?

At Changing Education, we use a number of cloud-based services. Where possible, we ensure that data is stored within the EEA (https://www.gov.uk/eu-eea). An example of this is our use of an AWS environment that is hosted in Ireland. There are some instances where we have had to utilise the services of countries that are not in Europe, or who are not a trusted country. These are listed in our Privacy Policy on our company website (https://changingeducation.co.uk). This describes the measures that these organisations take to ensure that data is kept safe and secure.

In the event that we need to 'relocate' any data, we will update this policy and inform the contact that we have on file for the Education Provider.

If you require more information then please contact our Data Officer, Stephen Hackney.

6. What happens if the data is breached? How will I know?

The Information Commissioners website describes a breach as:

> *A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.*

While we have taken a number of organisational and technical measures to ensure that your data is not breached, we recognise that there are no guarantees in life. Therefore, we have developed a Incident management process to ensure that where we are required to do so, we will notify the Data

Controller of any breaches that may occur. We will inform the named person that we have on our system. We would ask that if you wish us to notify anyone else, that our Data Officer is informed in writing.

7. Will my data be processed by any third parties?

Yes, probably. Whether we are processing student data or just sending our customers an invoice, we have a requirement to share information with other organisations. We have documented these organisations in our Data Privacy Policy which is available on our website. If we need to change any of these processors, we will inform you. We have completed due diligence of all our third parties to ensure that they operate to the same levels of compliance as we do.

In a limited number of circumstances, we may need to share information with the authorities. This is one of our statutory obligations and where possible, we will inform the Data Controller before doing so.

More information is on the ICO website:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

8. What organisational and technical measures do you have in place?

We have a number of measures in place in addition to those already documented here. These include a number of supporting HR policies to ensure that every member of staff at Changing Education Group is aware of their responsibilities together with education and training which is provided on an ongoing basis. We also test our systems on an annual basis to ensure their integrity. Our Data Officer is responsible for ensuring that we treat the personal information of our Clients, staff and suppliers in the way that we would want our own data to be managed.

9. Why don't Changing Education group have a DPO?

A Data Protection Officer (DPO) is a role that is required by law for a small number of organisations. For Changing Education, it is not a mandatory requirement for us to appoint a DPO. However, this does not mean that we don't care about what happens to data or are negligent on how personal information is processed. Instead of appointing a DPO, we have appointed one of our Directors, Stephen Hackney, to be the Data Officer for the organisation. Stephen's role is to ensure that we are complying with appropriate legislation, ensuring that we have robust systems in place and staff who are knowledgeable and informed.

Finally, we are working closing with a specialist organisation called Risk Evolves who have DPO resource should the need arise.

More information on Data Protection Officers:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

10. What happens at Brexit ?

Good question ! There is still uncertainty on whether the UK will achieve adequacy, and like all organisations we are monitoring the path of Brexit negotiations. However, as part of our preparation we have mapped (Record of Processing Activities or ROPA) our data and understand where information is being processed and why. We have reviewed our contracts for those suppliers outside of the UK and have standard contract clauses in place with them (this is documented in our Privacy Policy). We do not believe that the end of the transition period will have a major impact on our services and will notify if we identify any issues.

More information is available on the ICO's website:

https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/

11. Where do I go to find out more?

If you have any queries on anything in this document, then please contact our Data Officer at s.hackney@changingeducation.co.uk