What action are you taking to prepare for the GDPR?

- We have appointed a DPO for the company. They have reviewed the Policies, Procedures and Products we provide and advised improvements based on the GDPR statement. Changes and requirements are outlined below:
- Changes to the Content Management System (CMS - Website Editor) have been made to allow for increased productivity when dealing with GDPR related areas. These include
    - A cookie bar can now be included which can be defined by the client. This also includes the ability to add known cookies to a list which is output in a privacy policy page which is now included in the CMS by default. This cookie list contains a list of predefined cookies sets that are common on our websites but also provides the option to add new ones.
    - Data submitted to form data, regardless of content, is encrypted where stored in a database.
    - Any user account data which is personal in nature is encrypted within the database.
    - Appointment of a DPO as a CMS user. The CMS will inform the DPO user where a person has not logged in to the CMS for a period of 6 months.
    - Upon termination of the website agreement with e4education all personal data is removed from the websites storage. This includes, user account data, form submission data and associated files the website is then archived. This archive is stored for a period of 3 months after agreement termination.

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

- Technical
    - The access to majority of our servers requires the use of public and private encryption keys. For those that require just passwords are restricted to a high level of complexity and restricted to authorised IP addresses only.
    - VPN access is restricted to authorised employees only. Requires the use of public and private keys along with usernames and complex passwords.
    - Transmission of data is secured using SSL.
    - Storage of personal data or has the potential to be personal data within the website database is stored using encrypted data.

- Organisational
    - Only authorised staff have access to the data and all access requires valid credentials.

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

- The access to majority of our servers requires the use of public and private encryption keys. For those that require just passwords are restricted to a high level of complexity and restricted to authorised IP addresses only.
- VPN access is restricted to authorised employees only. Requires the use of public and private keys along with usernames and complex passwords.
- Only authorised staff have access to the data and all access requires valid credentials.
- E4education employees have participated in GDPR training.
- E4education employee contracts outline a strict confidentiality clauses relating to data protection.

How secure are your systems?

- Website Services

- Anti-Virus (AVG corporate and Sophos combination) are updated Daily with new definitions and Firewalls. Use of both Hardware (Cisco 5515 ASA Hardware firewalls) and Software based firewalls.
- Transmission between Site and servers and visitors to the website uses SSL.
- Use of Detectify CMS security testing to test website security and vulnerabilities.
- Backups of data taken for disaster recovery purposes only. Full backups taken weekly with incremental daily backups. Backups are stored on site at our London Data Centre and destroyed after 3 months.

Do you have any information management accreditation?

- No

Points below will be covered by updated Client Website Agreement which will be sent out to all clients within the next few days.

- The subject matter, duration, nature and purpose of the processing
- The type of personal data being processed
- The categories of the data subjects
- The obligations and the rights of the data controller (the school)
- That the data processer (you, the supplier) processes data only on the documented instructions of the school
- That the people who process the data are committed to confidentiality
- That you take measures to ensure secure processing
- That you will not engage another processor without prior written authorisation from the school, and that if you do so, that processor will also be bound by the same data protection conditions as are in your contract with us
- That you help the school comply with requirements regarding the data rights of individuals (e.g. to access, delete or rectify data), secure processing, the reporting and communication of data breaches, and the conducting of impact assessments where relevant
- That you delete or return the personal data to the school at the end of your provision of services
- That you make information available to us to demonstrate your compliance with the obligations in our contract, and allow us or a third party instructed by us to conduct audits and inspections