Code of Conduct

Last reviewed 1 Nov 2023

Glossary of Terms

Data Controller is the registered school, School Sport Partnership (Inc. School Games Organiser) or Active Partnership who supplies the survey for data collection

Data Processor is Seamless Software
Company Number 10086503
ICO Ref:ZA391440

Details of Processing

- Overview - the processor may only process personal data in line with the controller's documented instructions
    - Koboca holds data relating to surveys answered by pupils of school age. This includes school name, year group, gender and name - as the system can be configured by each school to include additional questions this data set may be extended. The data is used to populate reports to allow schools to collate pupil's views and test scores and identify target groups to offer support.
- The nature of the processing is a health and wellbeing and physical activity
- The type of personal data collected and stored is the gender, year group and how much physical activity a pupil does
- The controllers obligations are:
    - To ensure they have the necessary legal basis for processing the data
    - To only make written requests to Seamless Software in relation to data processing
    - To never ask Seamless Software, or use the Koboca system, to process data in a way which would breach any obligation under the Data Protection Act 2018, and the GDPR from 25 May 2018)
    - To undertake a data protection impact assessment before requesting, or making, changes to data processing
    - The controller retains overall control of the data provided to the processor
- Our obligations as a Data Processor when we process data on your behalf
    - To refuse requests relating to data processing unless it is made in writing
    - To refuse a request to change data processing where we are aware it would breach any obligation under the Data Protection Act 1998 (up to and including 24 May 2018, and the GDPR from 25 May 2018)
    - To provide assistance, where necessary, to allow you as the Data Controller to discharge your duties to allow data subjects to exercise their rights under the Data Protection Act 1998 (up to and including 24 May 2018, and the GDPR from 25 May 2018)
    - To notify and obtain authorisation form the Data Controller where we are aware that a requested change to the data processing is likely to impact the risk level of data processing
    - From 25 May 2018 - To provide you (as the Data Controller) with information, files and documentation as required to ensure both parties are meeting their GDPR Article 28 obligations. Where necessary to submit information, files

and documentation to allow the Data Controller to inspect or audit the data processing

- If a processor acts outside of the controller's instructions in such a way that it decides the purpose and means of processing, including to comply with a statutory obligation, then it will be considered to be a controller in respect of that processing and will have the same liability as a controller

Terms

The following terms are in accordance with Article 28(3)

- Processing only on the documented instructions of the controller.
- Seamless Software work to ensure all data is only kept for the period it is required within the following factors.
    - Legal retention period: For data with a legal requirement including accounting, employment and administrative law, this data will be held for the period required under the relevant legislation.
    - Contracted period: For data which is processed for the purpose of providing a service within a contracted period, the data will be maintained for the agreed period

Both controllers and processors are obliged under Article 32 to put in place appropriate technical and organisational measures to ensure the security of any personal data they process

- Access to the Koboca system is secured through the use of a secure logon system, and all internet traffic is sent over a securely encrypted TLS 1.3 / HTTPS connection. We also ensure that all sensitive information is encrypted at rest using AES256 and all our servers are securely hosted in the UK, managed by our technology partner See Green (see Data Sub-processors). As a user of the system, schools need to ensure they maintain the security of their login details and should notify Seamless Software immediately if they believe there login details may have been compromised

- Seamless Software recommend schools only access data through their secure school networks. Schools should ensure they log out of Koboca whenever leaving their computer unattended. Seamless Software recommend schools should not print out any names or sensitive data. Login details should be kept safe and not shared with colleagues, any breach of security should be reported to Koboca immediately. Seamless Software advise schools to ensure screenshots, login details or other data taken from the Koboca system to be held in a secure location.

  Only teachers working under the duty of statute in a school will be given secure logins and access to data with the school account, which is only accessible using the random strong password provided by Seamless Software. Staff should not change the password unnecessarily, or re-use existing passwords

- Schools are advised to get parental/guardian consent before pupils complete any surveys on the Koboca system
- Request can be made to remove data and when we receive a data removal request relating to data we are the Data Processor for, we will pass that request to the relevant Data Controller within 24 hours. We will not action any data removal request

without the relevant Data Controllers authorisation, except in any instance where we are legally obliged to do so.

- The controller has the right to make a request of the processor for subject access requests, requests for the rectification or erasure of personal data, and objections to processing, and these will be dealt with in a timely manor
- The controller has access to their own data via a secure login. FAQ's are available on the website www.koboca.co.uk and Seamless Software staff are available to provide support
- Where a contracted processing period has ended, we will automatically delete the data in line with our removal procedure, unless we have a prior written request from the Data Controller to return the data to them at the end of the contract. Where a data return is requested, we will arrange for a secure data transfer to the Data Controller. Once safe receipt is confirmed the data will be deleted in line with our removal policy. Data deletion will occur on live systems within 10 working days of passing the required retention period, and 90 days on backup systems.
- When data is no longer required for the original purpose of processing, the contract period has ended, or the subject has withdrawn consent to processing their data, all personal data will be deleted from our system, except in cases where we are required to retain that information for contractual, accounting or legal reasons. If consent for data processing is withdrawn for data, we are unable to delete, due to accounting or legal reasons, the party wishing to withdraw consent will be notified within 5 working days.

Audit - Under Article 28(3)(h):

- the processor to provide the controller with all the information that is needed to show that the obligations of Article 28 have been met; and
- the processor to allow for, and contribute to, audits and inspections carried out by the controller, or by an auditor appointed by the controller.

To demonstrate compliance with the whole of Article 28 to the controller. We will do this by giving the controller the necessary information requested

As processor we will assist the controller in meeting its obligations to:

- keep personal data secure;
- notify personal data breaches to the ICO;
- notify personal data breaches to data subjects;
- carry out data protection impact assessments (DPIAs) when required; and
- consult ICO where a DPIA indicates there is a high risk that cannot be mitigated.

At the end of the contract the processor must:

- at the controller's choice, delete or return to the controller all the personal data it has been processing for it; and
- delete existing copies of the personal data unless UK law requires it to be stored.

Deletion of personal data will be done in a secure manner, in accordance with the security requirements of Article 32.

The contract must include these terms to ensure the continuing protection of the personal data after the contract ends. This reflects the fact that it is ultimately for the controller to decide what should happen to the personal data being processed, once processing is complete.