Sentinus
Science Technology Engineering Mathematics

General Data Protection Regulation (GDPR)

Sentinus Policy

Sentinus Background

Sentinus is an educational charity and company limited by guarantee. It engages young people, aged 5 – 19 years, in STEM (science, technology, engineering and maths) enhancement and enrichment activities and supports the development of links between schools, young people, industry, academia and public sector organisations.

To facilitate the execution of its aims it is necessary for Sentinus to collect and record information on its programme participants, in accordance with the General Data Protection Regulation (GDPR) May 2018.

General Data Protection Regulation (GDPR) Background

Sentinus is committed to a policy of protecting the rights and privacy of individuals, including, staff, participants in programmes, teachers, volunteers and others in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands transparency and accountability in how Sentinus manages and uses personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that Sentinus needs to be aware of as data controllers, including provisions intended to enhance the protection of personal data.

Sentinus needs to process certain information about staff, programme participants, volunteers, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- recruitment and payment of staff, associate staff and support staff;
- administration for programmes;
- student applications and registrations for programmes;
- volunteer registration for supporting programmes;
- contractual obligations with funders to gather data.

To comply with its legal obligations, including those imposed by the General Data Protection Regulation (GDPR), Sentinus must ensure that all information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Compliance

This policy applies to all Sentinus staff and associate staff. Any breach of this policy, or of the Regulation itself, will result in disciplinary action. As a matter of best practice, other agencies

and individuals working with and for Sentinus will be expected to read and comply with this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

The GDPR legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living persons, including children, by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

For more detailed information on these regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO) at www.ico.gov.uk

Responsibilities Under the GDPR

Sentinus appoints the Chief Executive to be the 'data controller' under the terms of the legislation – this means responsibility for controlling the use and processing of personal data. The data controller determines the purposes and means of processing personal data and ensures Sentinus 'data processors' comply with the GDPR and encourages good information handling within Sentinus. Compliance with the legislation is the personal responsibility of all Sentinus staff who are 'data processors' and process personal information. Individuals who provide personal data to Sentinus are responsible for ensuring that the information is accurate and up-to-date.

The Chairman of the Sentinus Board of Trustees is appointed SIRO (Senior Information Rights Owner) to set and approve formal policies and ensure the 'Data Controller' is given suitable guidance and is following this correctly.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with eight principles. In order to comply with its obligations, Sentinus undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

Sentinus will make all reasonable effort to ensure that individuals who are the focus of personal data (data subjects) are informed of:

- the identity of the data controller;
- the purpose of processing data;
- any disclosures to third parties that are envisaged;
- the period for which the data will be kept;
- any other information which may be relevant.

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

Sentinus will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

Sentinus will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4) Keep personal data accurate and, where necessary, up to date.

Sentinus will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify Sentinus of any change in circumstance which means that data needs to be updated. It is the responsibility of Sentinus to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

Sentinus undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. Sentinus will undertake a regular review of information held and implement a data removal process, if necessary. Sentinus will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

The rights of individuals under the legislation include:

- the right to be informed of the nature of the information held and any parties to whom this may be disclosed;
- the right of access to the information held;
- the right to rectification if data held is inaccurate;
- the right to have data removed and/or destroyed;
- the right to restrict processing of data;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

Sentinus will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.
Sentinus, and its employees, are responsible for ensuring that any personal data held is kept securely and not disclosed to unauthorised third parties. Sentinus will ensure that all personal data is accessible only to those who have a valid reason for using it.

Sentinus will have in place appropriate security measures:

- keeping all hard copy personal data in a lockable cabinet with key-controlled access;
- password protecting personal data held electronically;
- archiving personal data which are then kept securely;
- ensure data on digital equipment is not visible except to authorised staff;
- ensuring that computer screens are not left unattended without a password protected screen-saver being used.

In addition, Sentinus will put in place appropriate measures for the deletion of personal data Hard copy records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant computers will be wiped clean before disposal or physically destroyed. A log will be kept of records destroyed.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Sentinus will not transfer data to such territories without the explicit consent of the individual.

Consent as a Basis for Processing

In pursuit of its aims, Sentinus will only hold personal data if the subject has given their consent.

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when Sentinus is processing any sensitive data, as defined by the legislation.

Sentinus understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from non-response to a communication.

In pursuit of its mission Sentinus needs to collect and hold information on:

- staff and associate staff;
- programme participants (students);
- teachers;
- sectoral ambassadors and industry/employers representatives;
- parents/guardians;
- funders/sponsors;
- other people in connection with delivery of Sentinus activities.

Sentinus will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by Sentinus. Any individual wishing to exercise this right should apply in writing to the Chief Executive. Any member of staff receiving a SAR should forward this to the Chief Executive. Under the terms of the legislation, any such requests must be complied with within forty days.

Disclosure of Data

Sentinus undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police. Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure;
- the disclosure has been notified to the OIC and is in the legitimate interests of Sentinus;
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.

Policy Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998. For further information on GDPR please go to the Information Commissioner Office (ICO) website www.ico.gov.uk b which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.