The KEVIET Trust

GDPR Data Protection Policy

Author: James Lascelles
Designation: Headmaster
Date: May 2018

Date approved : May 2018
Committee Chair : Andrew Harrison
Next review Date: May 2021

Contents:

Statement of intent

King Edward VI Education Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other Trusts and educational bodies, and potentially children's services.

This policy is in place to ensure all staff, governors and trustees are aware of their responsibilities and outlines how the Trust complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and King Edward VI Education Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
    - The Freedom of Information Act 2000
    - The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
    - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as a name, an identification number or an online identifier such as an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters and racial or ethnic origin.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. King Edward VI Education Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy notices.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of high risk processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used for High Risk activities as specified and defined under the term of the GDPR.

5. Roles and Responsibilities

5.1. The Trust will appoint a Trustee or Trustees to the position of DPO who will be responsible for auditing and monitoring the Trust's compliance with the GDPR.

5.2. The Headmaster or delegated member of the SLT will be responsible for raising awareness and organising training for staff on their obligations under the GDPR

5.3. The Clerk to the Governors will be responsible for supporting the DPO with processing of Subject Access Requests.

5.4. The Headmaster's PA will be responsible for effecting any changes or directing others to remove inaccuracies, subject removal or other such changes as a consequence of a query, complaint or subject access request.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

6. Lawful processing

6.1. The legal basis for processing data will be identified and published in the school's GDPR Privacy Notice.

6.2. The Trust will act as a data processor; however, this role may also be undertaken by third parties.

6.3. Under the GDPR, data will be lawfully processed under one or more of the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.

- Processing is necessary to protect the vital interests of a data subject or another person.

6.4. Sensitive data is defined under the GDPR as racial or ethnic origins; political or religious beliefs; trade union activities; physical or mental health or criminal activities.

6.5. Sensitive data is only be processed by the school where:

- Explicit consent of the data subject has been received.
- Processing relating to personal data that has already been manifestly made public by the data subject and is already in the public domain.
- Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law.
- Protecting the vital interests of a data subject.
- The establishment, exercise or defence of legal claims and/or investigations relating to legal claims or potential legal claims.
- The purposes of preventative or occupational medicine, for assessing the capacity of the employee or pupil, confirming medical diagnosis and determining reasonable adjustments to support the individual.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, *acceptable consent already obtained from parents of current children and staff under the DPA will not be reobtained.*

7.2. The Trust will ensure that new consent mechanisms meet the standards of the GDPR and with effect from the 1st September 2018 will begin collecting new consents from new students entering the school: any renewed consents will be completed in line with GDPR and on new consent forms.

7.3. Where the processing of data is not specified in our privacy notices and cannot be done so under any other lawful basis the school will request explicit consent.

7.4. Consent can be withdrawn by the individual at any time.

8. The right to be informed

8.1. The Trust will publish an accessible privacy notice for parents, pupils and staff on its website and will update this from time to time as necessary in line with the GDPR

8.2. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.3. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.4. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.5. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. The school recognises and follows the ICO's code of practice for SAR and their best practice advice this includes:

- The publication of an accessible form downloadable from the school's website to efficiently monitor and administer SAR.
- This form contains a separate section to verify the identity of the person making the SAR in order to fulfil our safeguarding obligations and our duties under the FOI; GDPR and Data Protection Acts: acceptable proofs of identify include electronic or photocopied scans of either driver's license and/or passports.

9.2. A hard copy of the information will be supplied to the individual free of charge and posted to their address as further security of proof of identify; the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.3. Where information is voluminous or requires additional explanation then the school will arrange with the request a mutually convenient time for onsite viewing.

9.4. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.5. All fees will be based on the administrative cost of providing the information

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

10.3. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.3. The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the Trust's processing of personal data.

12.2. In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The Trust will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The Trust will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

13.9. The Trust will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing

- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

14.6. Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

15. Automated decision making and profiling

15.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

15.2. The Trust does not make any decisions based on automated processing.

16. Privacy impact assessments

16.1. Data protection impact assessments (DPIAs) will be used in line with the GDPR guidance for areas of "high risk" to help the Trust identify the most effective method of complying with the Trust's data protection obligations in areas of high risk.

16.2. A DPIA will only be carried out when using "high risk" technologies when processing is likely infringe the rights and freedoms of individuals.

16.3. The school only carry's out the following routine areas of data collection that could potentially be identified as "high risk"

- Biometric scanning for cashless catering provided by a GDPR compliant third party.
- Onsite CCTV [see section 19]
- CRB and DBS checking for criminal records carried out by a GDPR compliant third party.

16.4. The school does not and has no plans to carry out any of the high risk activities as identified in the GDPR Act.

17. Data breaches

17.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

17.3. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

17.4. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.5. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18. Data security and Records Management

18.1. The following items are classified as confidential and must be securely stored and not *accessible* or *published* to unauthorised persons:

- **All** student records in whatever format.
- **All** staff records in whatever format.

- **All** parent records in whatever format.
- **All** Finance/HR and Payroll records in whatever format.
- **All** other school records that could potentially contain personal data or sensitive commercial data.

18.2. The staff have different levels of access to data dependent upon the individuals role in the school and their requirements to access specific data related to their role.

18.3. Where personal information that could be considered private or confidential is taken *off the premises*, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. using encrypted memory sticks; accessing information via the secure staff/pupil portal; taking extra-care with confidential papers/records.

18.4. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

18.5. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust premises containing sensitive information are supervised at all times.

18.6. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on an ongoing basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.7. The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19. CCTV and Photography

19.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

19.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via this policy; and notices around the site.

19.3. CCTV footage will be kept for six months for security purposes; the Facilities and Estates Manager is responsible for keeping the records secure and allowing access.

19.4. The school only processes CCTV footage for the purposes of collecting evidence in the cases of a behavioural incident or monitors students behaviour via live CCTV footage [non-processing]

19.5. The Trust captures consent for the use of students images either still or video for marketing purposes on the schools website; related news articles in the local

papers and on our Twitter and Facebook feeds. Parents, staff and students have the right to alter amend or remove their consent at any time by contacting Rhona Adam. rhona.adam@kevigs.lincs.sch.uk

20. Data retention

20.1. Data will not be kept for longer than is necessary.

20.2. Unrequired data will be deleted as soon as practicable.

20.3. Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

20.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained

21. DBS data

21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

21.2. Data provided by the DBS will never be duplicated.

21.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

22. Policy review

This policy is reviewed every three years by the Headmaster.

The next scheduled review date for this policy is May 2021.