Youth Engagement Schools Trust

Data Protection Policy

Approved by: Board of Trustees
Reviewed by: Chris Heptinstall & Nic Brindle
Latest Policy review: Spring 2024 – Full Board Meeting – 18th April 2024
Next Policy review date: Spring 2025

Introduction

The Youth Engagement Schools Trust (YES Trust) will comply with the demands of the General Data Protection Regulation (GDPR), and the Data Protection Act 2018 The Trust regards the security of personal data as one of its most important responsibilities, and will constantly review and improve processes and procedures to ensure that personal data is only viewed by those that need it.

Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction, and further CPD. All staff undertake annual online Data Protection training as part of the Trust's ongoing work to protect personal data.

This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The Trust is a Data Controller as data is processed, that is the personal information of pupils, families, staff, visitors and other Trust users.

The Trust is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

Definitions

Data processing
The acquisition, storage, processing and transmission of data.

Data subject
Any identifiable person whose data is held or processed.

Consent
Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available for an audit. A person must be 13 years old in order to record their consent.

Cross-border processing
The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area).

Sensitive data
The GDPR/ICO requires that particular care is taken with the following data

- Data regarding children
- Health (physical, mental, genetic)
- Ethnicity
- Religion
- Sexuality
- Performance management and trade union membership

Filing system

Any structured set of personal data, however stored in any format (physical or digital) that can be processed.

Personal data breach
A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation
The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

Password protection
The act of 'locking' a device or document. The information remains readable beyond the password.

Encryption
The act of encoding all the information beyond a password or code.

Legal basis
The Trust decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties the Trust uses the following bases for processing and controlling data:

Legal basis: **Public Task**

- Admissions
- Attendance
- Assessment
- Pupil and staff welfare
- Safe recruitment
- Staff training
- Performance Management

Legal basis: **Consent**

- Various uses of photographs and moving images
- Trade union membership
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement)
- The use of data to promote the social life of the Trust community

Legal basis: **Contract**

- When processing is required to carry out the performance of a contract

Personal data
Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

Data portability, data subject access request

Data subjects (or a child's parents/carers) may request access to a copy of all their data. The Trust has established an efficient means of accomplishing this task which may not carry a charge and will be completed within one calendar month, after the next working day. Data subjects may request that data is brought up-to-date or made more accurate.[1]

Principles

- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up-to-date
- Personal data may identify the data subject only as long as is necessary for processing
- Personal data must be processed in a manner that ensures its security
- Any breaches in data security must be reported to the ICO within 72 hours
- The Trust must report any breaches caused by third parties who have access to Trust users' data within 72 hours
- The Trust must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information

Roles and Responsibilities

The Trust/academy Privacy Statements set out in detail how the Trust will maintain the security of users' data. The Acceptable Use Policies set out the duties of the staff and other Trust users in supporting data security.

Within each academy the security of data is coordinated by the Headteacher, supported by The Director of Business and the Chief Executive Officer.

All staff are responsible for:

1. Collecting, storing and processing any personal data in accordance with this policy
2. Informing the school of any changes to their personal data, such as a change of address
3. Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice or deal with data protection rights invoked by an individual

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Headteachers

Responsible for ensuring data protection policy and procedures are being adhered to within their schools. Headteachers cannot delegate their accountability for the practice in their schools, and should be leading by example and always being aware of how adherence is in their settings.

Senior Leaders

Responsible for supporting the Headteacher in their responsibilities and ensuring staff and themselves are adhering to policy and procedure

Office Managers

Responsible for ensuring office documentation and all personal data held on site is safe and secure and being processed and held in line with our privacy notices and acceptable use policy. Office Managers are also responsible for coordinating responses to SAR's, DPIA's and FOI requests, and will in most cases be the main link between the school and the Trust DPO.

Admin Staff

Responsible for keeping personal data in the school office safe and secure, and ensuring they are working with the highest regard to data protection, particularly in school offices where pupils, visitors and staff may be in close proximity (being able to view for example) personal data.

Teaching and Support Staff

Responsible for ensuring any personal data that they access and use is kept safe and secure, and making sure they are considering data protection with all their teaching practice. Teachers should also consider data protection in relation to using new systems and processing, including having an understanding of DPIA's/

Trust Board

The trustee with special responsibility for data security is Robert Halsall. The Board of Trustees is responsible for ensuring there is a fit for purpose Data Protection Policy and that it is being implemented correctly, through visits to schools, reports from ELT, and external audit reports.

The Trust has appointed a **Data Protection Officer** who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the Trust Executive Leadership and Senior Leaders within its academies and support the Trust with updates and interpretations as the GDPR develops.

The DPO will liaise between the Trust and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the Trust in its communication with schools' users (pupils, families, parents, governors, contractors and visitors) about the school's GDPR

procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects' rights.

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

1. Confirmation that their personal data is being processed
2. Access to a copy of the data
3. The purposes of the data processing
4. The categories of personal data concerned
5. Who the data has been, or will be, shared with
6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
7. Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
8. The right to lodge a complaint with the ICO or another supervisory authority
9. The source of the data, if not the individual
10. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
11. The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to the DPO and include:

12. Name of individual
13. Correspondence address
14. Contact number and email address
15. Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

1. Withdraw their consent to processing at any time
2. Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
3. Prevent use of their personal data for direct marketing
4. Object to processing that has been justified on the basis of public interest, official authority or legitimate interests

5. Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
6. Be notified of a data breach (in certain circumstances)
7. Make a complaint to the ICO
8. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Data Protection Officer

Chris Heptinstall
dob@theyestrust.org
07394566490

Staff should contact the DPO should they believe that this policy and/or the privacy statements and/or the acceptable use policies are not being followed.

Data Audit

The Trust will carry out an annual data audit. Within the audit the Trust will record all third parties' compliance with GDPR if those third parties process data for any school/Trust users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of school users' data is involved. The Trust will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.

Preferably companies that process school users' data will have certification to ISO27001.

The audit will also check the security of physical and digital records and devices.

Processing Records

To meet the ICO's recommendation that 'scrupulous records' are developed the Trust will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any Trust user data will be recorded.

In broad terms the Trust will record which data has been processed (including deletions when data should no longer be stored) and on which legal basis.

Consent replies are recorded within the system.

Sharing Data

Personal data may be shared with third parties to;

- Protect the vital interests of a child
- Protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC (HM Revenue and Customs)

CCTV

CCTV is used to support the safety and security of academy users in Trust settings. We adhere to the ICO's code of practice for its use. Although consent is not required for its use, prominent notices inform setting users/visitors that CCTV is used within each school site where applicable.

Photographs and moving images

Consent is requested from parents and staff for the use of images. Letters requesting consent outline the choices that pupils and staff may make for the use of their images.

The school may seek consent to use photographs for the following purposes:

- To support school user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the school
- To celebrate achievement in the printed press
- To celebrate achievement online

Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The YES Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the YES Trust/school will treat this as a data breach and will follow the personal data breach procedure as outlined in this policy.

Desks, Screens and Paperwork

Whilst it is the intention of the Trust and its schools to use as little paper as possible, the Trust recognises that this is not always possible or realistic – particularly with finance staff dealing with receipts, orders, invoices, and certain pupil records that come from prior schools. The Trust will however ensure that no documents containing personal or sensitive information are left out whilst a desk is unattended, or after a staff member has gone home for the day, even if their office is locked. All documents containing personal/sensitive information being worked on, must be locked away at the end of the working day.

Laptops and display screens must be locked when not in use, or when a staff member is away from their device, no matter how short a time they might be away from it for. Should a staff member have concerns about others viewing their screen (whether that be pupils, staff or visitors), they should talk to the Office Manager about ways to mitigate this. This may include changing the position of monitors to face away from public areas, adding privacy screens to desks, or adding a privacy screen to their monitor.

At the end of a school/working day, all desks and work areas must be clear of all personal/sensitive information and documentation, and staff should endeavor to keep a clear desk as much as possible throughout the day, but especially when they have finished work.

Should a staff member require a lockable desk/drawer/locker in order to facilitate this, then they should speak to the Office Manager in the first instance.

The school's specific data security measures - data protection by design

A. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.
B. All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server room locked when the school is closed and at other times of reduced security; desktop computers and portable devices will be sited/stored in secure places.
C. Staff are expected to ensure the safety of their allocated school devices: devices may not be left unattended in cars at any time, and they must be kept out of sight if taken home.
D. All passwords must be 'strong;' (at least 8 characters with a mixture of upper and lower case letters, numbers and symbols), the Trust will require regular changing of passwords.
E. No passwords will be written down or shared; advice is available on the safe storage of passwords.
F. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.
G. Devices that are used to process sensitive data and/or are vulnerable to theft should be secured with encryption.
H. All emails containing personal data will use school systems and be encrypted
I. All deleted data will be deleted in a secure manner: physical data will be shredded, and digital data will be fully deleted with trash / junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by Owness Solutions.
J. Only data that is necessary for the effective performance of the school will be processed.
K. Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).
L. Staff will be updated with any significant interpretations or developments of the GDPR.
M. The school will have data impact assessments in place to protect vulnerable data subjects and sensitive data.
N. Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.
O. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a school user's needs, but not to others. Physical records must always be stored in locked cabinets, in office/admin areas where access is also restricted.

P. All school users will handle personal data with care: it will not be left unattended (unattended computers must be locked), school users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.

Q. All computers that might be used to process data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.

R. The headteacher and/or the DPO will approve who and how personal data is stored on mobile devices.

S. All digital data that is stored will be backed up on at least password protected devices.

T. Personally owned devices will not be used for the storage of school personal data.

Data breaches

All staff must report to a member of the SLT or the DPO any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for the SLT/DPO to decide whether to the suspected data breach warrants reporting to the ICO. A data breach would include the accidental sharing of personal data via a wrongly addressed email.

Training

All staff will receive basic training in the requirements of the GDPR via the Trust's online training platform. The training will be recorded in the data audit and/or the data processing records. Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The Trust will keep staff, trustees, and governors up to date with guidance, changes, and interpretations to data protection law.

Data Protection Impact Assessment (DPIA)

For any changes in the Trust's most sensitive data processing activities, the Trust will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the Trust's reputation. Staff involved in processing the school/Trust's most sensitive data will have to record their reading and understanding of the relevant DPIA.

Further Information on DPIA's is to be found in Appendix 1, including how to know when to complete one.

Monitoring

The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

Footnotes

1. Data subjects' rights include

- The right to be informed
- The right of access
- The right to object
- The right to be forgotten (this might prove impossible in the Trust context)
- The right of rectification (any inaccurate data must be corrected)

2. In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's

- Reputation
- Confidentiality
- Financial wellbeing
- A loss of control over their data
- Make them vulnerable to discrimination
- Their rights and freedoms

Links with other policies

This Data Protection Policy is linked to our:

- ICO Model Publication Scheme
- Freedom of Information - Publication Guidance
- YES Trust CCTV Policy
- YES Trust Online Safety Policy

All of these can be found on the Trust's website

https://theyestrust.org/governance/

Appendix 1 - Data Protection Impact Assessment (DPIA)

Staff should generally speak to the Office Manager or DPO in the first instance to see whether a DPIA is required, but in general, if we are changing the way we process personal data, then a DPIA must be carried out, and reviewed/approved by the DPO. This might include a new system for assessing pupils' reading ability that stores pupil names, for example.

The following is taken from the Information Commissioners Website:

What is the general rule?

Article 35(1) says that you must do a DPIA where a type of processing is **likely to result in a high risk** to the rights and freedoms of individuals:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

What does 'high risk' mean?

Risk in this context is about the potential for any significant physical, material or non-material harm to individuals. See What is a DPIA? for more information on the nature of the risk.

To assess whether something is 'high risk,' the UK GDPR is clear that you need to consider both the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk in that sense is part of the job of a DPIA.

However, the question for these initial screening purposes is whether the processing is **of a type likely to result in** a high risk.

What does 'likely to result in a high risk' mean?

The UK GDPR doesn't define 'likely to result in high risk.' However, the important point here is not whether the processing is actually high-risk or likely to result in harm – that is the job of the DPIA itself to assess in detail. Instead, the question is a more high-level screening test: are there features which point to the potential for high-risk? You are screening for any red flags which indicate that you need to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail.

Article 35(3) lists three examples of types of processing that automatically require a DPIA, and the ICO has published a list under Article 35(4) setting out ten more. There are also European guidelines with some criteria to help you identify other likely high-risk processing.

This does not mean that these types of processing are always high risk, or are always likely to cause harm – just that there is a reasonable chance they may be high-risk and so a DPIA is required to assess the level of risk in more detail.

If your intended processing is not described under UK GDPR, Article 35(3) the ICO list or European guidelines then ultimately, it's up to you to decide whether your processing is of a type likely to result in high-risk, taking into account the nature, scope, context and purposes of the processing. If in any doubt, we would always recommend that you do a DPIA to ensure compliance and encourage best practice.

What types of processing automatically require a DPIA?

Article 35(3) sets out three types of processing which always require a DPIA:

Systematic and extensive profiling with significant effects:

"(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."

Large scale use of sensitive data:
"(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10."

Public monitoring:
"(c) a systematic monitoring of a publicly accessible area on a large scale."

What other factors might indicate likely high-risk?

The Article 29 working party of EU data protection authorities (WP29) published guidelines with nine criteria which may act as indicators of likely high-risk processing:

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract.

For more guidance on these factors, read the WP29 guidelines (WP248). They give background on the reasoning for the high-risk indicators, and examples of processing likely to result in high-risk.

In most cases, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule.

You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high-risk, but you should document your reasons.

On the other hand, in some cases you may need to do a DPIA if only one factor is present – and it is good practice to do so.