



PETERBOROUGH KEYS
ACADEMIES TRUST

GDPR POLICY

Version 3.1

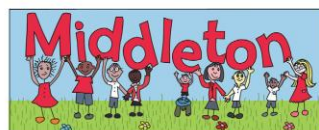
June 2022

Trustee Committee: Trust Board on 12 July 2022

Reviewed by DPO: 24 May 2022

Date Policy Reviewed: June 2022

Date of Next Review: June 2024



Contents

Paragraph.....	Page
1. Introduction.....	1
2. Aims.....	1
3. Legislation and guidance	1
4. Definitions.....	2
5. The data controller.....	3
6. Roles and responsibilities.....	4
7. Data protection principles	6
8. Collecting personal data.....	7
9. Sharing personal data.....	8
10. Subject access requests and other rights of individuals.....	9
11. Parental requests to see the educational record.....	12
12. Biometric recognition systems	12
13. CCTV.....	13
14. Photographs and videos.....	13
15. Data protection by design and default.....	14
16. Data security and storage of records.....	15
17. Disposal of records.....	15
18. Personal data incidents.....	16
19. Training	16
20. Monitoring arrangements.....	16
21. Links with other policies	17
22. Version History.....	17

1. Introduction

- 1.1 This policy is managed and maintained by the Chief Operating Officer (“COO”) supported by the Trust’s Data Protection Officer (“DPO”) with ratification through the Trust Leadership Group prior to presentation for Trustee approval.
- 1.2 The policy has been developed in order to demonstrate the principles and approaches of the schools comprising the Peterborough Keys Academies Trust (“PKAT”), and the Trust itself, regarding the General Data Protection Regulations (“GDPR”) that came into force across the United Kingdom on 25 May 2018.

2. Aims

- 2.1 Our Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).
- 2.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Legislation and guidance

- 3.1 This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](#) and the ICO’s [code of practice for subject access requests](#).
- 3.2 This policy meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data, which is used within some of our member schools for identification purposes.
- 3.3 This policy also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information. CCTV policies approved by Local Governing Bodies may exist at school level where CCTV is used within the school, providing further detail on how each school manages its CCTV infrastructure.

3.4 In addition, this policy complies with our Master Funding Agreement and the PKAT Articles of Association.

4. Definitions

Term	Definition
<p>“Personal data”</p>	<p>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<p>“Special categories of personal data”</p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as the algorithms defined by finger imaging, retina and iris patterns), where used for identification purposes • Health – physical or mental and any medical information • Sex life or sexual orientation
<p>“Processing”</p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering,</p>

	retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
“Data subject”	The identified or identifiable individual whose personal data is held or processed.
“Data controller”	A person or organisation that determines the purposes and the means of processing of personal data.
“Data processor”	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
“Local Data Officer”	A person nominated within each school, by the school itself, appointed to act as a local point of contact with an understanding of the local processes and system, and of the GDPR. This person will support the outsourced DPO and the Trust’s lead, the <i>Trust Systems Lead: Security & Students</i> in determining overall compliance of the Trust and its schools with the GDPR.
“Personal data incident”	An incident or suspected incident of security compromise leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
“Trust Systems Lead: Security & Students”	An appointed individual within the Trust who leads the working group of <i>Local Data Officers</i> and acts as a principal point of contact with the outsourced DPO.

5. The data controller

- 5.1 Our Academy Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, often at school level. The Academy Trust holds the status of data controller with schools processing data under license.

- 5.2 The Academy Trust is registered as a data controller with the ICO and will renew a single registration on behalf of all schools annually or as otherwise legally required.

6. Roles and responsibilities

- 6.1 This policy applies to **all staff** employed by our Academy Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

- 6.2 The following definitions are highlighted:

(a) Board of Trustees

- (i) The Board of Trustees has overall responsibility for ensuring that our Academy Trust complies with all relevant data protection obligations.

(b) Data protection officer

- (i) The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and assisting with the development of related policies and guidelines where applicable. The DPO is outsourced.
- (ii) They will link with Local Data Officers appointed by and within each member school of the Academy Trust for the purposes of their work.
- (iii) They will provide the Trust's Leadership Group with the findings of an annual audit into the school level compliance with the principles and procedures related to the legislation around data protection.
- (iv) The DPO is to be notified and the Trust shall record all data incidents. The DPO will act as the main point of contact for the ICO.
- (v) Full details of the DPO's responsibilities are detailed in the Service Level Agreement.
- (vi) The Academy Trust's DPO is:

GDPR Sentry Limited

Unit 434 Birch Park, Thorp Arch Estate, Wetherby, LS23 7FG

Email: support@gdprsentry.com

Web: <https://gdprsentry.com/>

(c) Local Data Officers

- (i) Local Data Officers will be nominated by each member school within the Academy Trust and will assist the DPO with audit work relating to their own school.
- (ii) Local Data Officers will be expected to have a command and understanding of the process and procedures in place at school level.
- (iii) Local Data Officers will be expected to support the Trust Leadership Group respond to the audit findings of the DPO by assisting with the implementation of change at a local school level wherever applicable.
- (iv) Local Data Officers may, subject to circumstances, discuss local matters with members of the Trust Leadership Group and the DPO.
- (v) Local Data Officers will support Headteachers in the dealing with personal data incidents as required.
- (vi) Local Data Officers will work with the Trust Systems Lead: Security & Students to drive GDPR compliance within the Trust.

(d) Headteachers

- (i) The Headteacher of each member school of the Academy Trust acts as the representative of the data controller on a day-to-day basis.
- (ii) The Headteacher of each member school will play a significant role in the management of personal data incidents relating to their school, supported by their Local Data Officer and Trust staff as appropriate.

(e) Trust Systems Lead: Security & Students

- (i) The Trust Systems Lead: Security & Students role purpose is to develop and lead a systematic Trust approach to aspects of the IT Strategy, relating to Security and Students. Regarding GDPR the principal focus is evaluating the effectiveness of the Trust approach to GDPR as a lead Data Officer, liaising with Local Data Officers in schools to drive harmonised, systematised and consistent approaches.

(f) All staff

- (i) All staff employed by the Academy Trust are responsible for:
 - (A) Collecting, storing and processing any personal data in accordance with this policy

- (B) Informing the school of any changes to their personal data, such as a change of address
- (C) Contacting the DPO in the following circumstances:
 - 1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - 2. If they have any concerns that this policy is not being followed
 - 3. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- (D) Contacting their Local Data Officer in the following circumstances:
 - 1. If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - 2. If there has been a data incident
 - 3. Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - 4. If they need help with any contracts or sharing personal data with third parties

7. Data protection principles

7.1 The GDPR is based on data protection principles that our Academy Trust must comply with.

- (a) The principles say that personal data must be:
 - (i) Processed lawfully, fairly and in a transparent manner
 - (ii) Collected for specified, explicit and legitimate purposes
 - (iii) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
 - (iv) Accurate and, where necessary, kept up to date
 - (v) Kept for no longer than is necessary for the purposes for which it is processed
 - (vi) Processed in a way that ensures it is appropriately secure.

- 7.2 This policy sets out how the Academy Trust and its schools aim to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

- (a) We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
 - (i) The data needs to be processed so that the Academy Trust or member school can **fulfil a contract** with the individual, or the individual has asked the Academy Trust or member school to take specific steps before entering into a contract
 - (ii) The data needs to be processed so that the Academy Trust or member school can **comply with a legal obligation**
 - (iii) The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
 - (iv) The data needs to be processed so that the Academy Trust or member school, as a publicly funded authority, can perform a task **in the public interest**, and carry out its official functions
 - (v) The data needs to be processed for the **legitimate interests** of the Academy Trust or member school or a third party (provided the individual's rights and freedoms are not overridden)
 - (vi) The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- (b) For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
- (c) Where we offer online services to pupils, such as classroom apps deemed essential to a pupil's learning, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).
- (d) Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.2 Limitation, minimisation and accuracy

- (a) We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

- (b) If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
- (c) Staff must only process personal data where it is necessary in order to do their jobs.
- (d) When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#)

9. Sharing personal data

9.1 We will not normally share personal data with anyone else, but may do so where:

- (a) There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- (b) There is an issue with a pupil or parent/carer that in our professional opinion puts the safety of the pupil at risk and therefore we have a statutory duty to refer to the appropriate body
- (c) We need to liaise with other agencies – we may need seek consent as necessary before doing this
- (d) Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - (i) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - (ii) Obtain a data sharing policy or statement from the supplier or contractor, either in the services contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - (iii) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- (e) We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
 - (i) The prevention or detection of crime and/or fraud
 - (ii) The apprehension or prosecution of offenders
 - (iii) The assessment or collection of tax owed to HMRC

- (iv) In connection with legal proceedings
- (v) Where the disclosure is required to satisfy our safeguarding obligations
- (vi) Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- (f) We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- (g) We may share personal data with the Department for Education, examination boards and the Local Authority in accordance with our statutory duties
- (h) We may send and receive data held on the Management Information Systems of our schools to other schools outside of our Trust, the Local Authority and the Department for Education in line with our statutory responsibilities.
- (i) Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

- (a) Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:
 - (i) Confirmation that their personal data is being processed
 - (ii) Access to a copy of the data
 - (iii) The purposes of the data processing
 - (iv) The categories of personal data concerned
 - (v) Who the data has been, or will be, shared with
 - (vi) How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
 - (vii) The source of the data, if not the individual
 - (viii) Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- (b) Subject access requests may be made in writing (by letter or email), verbally or via social media. A third party may also make a subject

access request on behalf of another person. Subject access requests may be submitted to the school. Requests should include:

- (i) Name of individual
 - (ii) Correspondence address
 - (iii) Contact number and email address
 - (iv) Details of the information requested
- (c) If the DPO receives a subject access request, they may pass it on to the Local Data Officer for attention at a school level, with the school's Headteacher also informed. If staff receive a subject access request, they must immediately forward it to the Local Data Officer.
- (d) The Local Data Officer shall proceed with attending to the request at school level. The Trust Systems Lead: Security & Students and Chief Operating Officer shall be made aware and will attend to the matter if it relates to whole-Trust activity.

10.2 Children and subject access requests

- (a) Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
- (b) Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil where that pupil is under the age of 12. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis
- (c) Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may not be granted without the express permission of the pupil where that pupil is over the age of 12. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to subject access requests

- (a) When responding to requests, we:
 - (i) May ask the individual to provide 2 forms of identification
 - (ii) May contact the individual via phone to confirm the request was made

- (iii) Will respond without delay and within 1 month of receipt of the request
 - (iv) Will provide the information free of charge unless our costs incurred in responding are considered unreasonable or excessive
 - (v) May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- (b) We will not disclose information if it:
- (i) Might cause serious harm to the physical or mental health of the pupil or another individual
 - (ii) Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
 - (iii) Is contained in adoption or parental order records
 - (iv) Is given to a court in proceedings concerning the child
- (c) If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
- (d) A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
- (e) When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 Other data protection rights of the individual:

- (a) 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 (see section 7), individuals also have the right to:
- (i) Withdraw their consent to processing at any time (however such a request may not be able to be fully met as we will be compelled to process in-line with our statutory duty)
 - (ii) Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
 - (iii) Prevent use of their personal data for direct marketing
 - (iv) Challenge processing which has been justified on the basis of public interest
 - (v) Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- (vi) Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- (vii) Prevent processing that is likely to cause damage or distress
- (viii) Be notified of a data incident in certain circumstances
- (ix) Make a complaint to the ICO
- (x) Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- (xi) 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. The DPO may pass such requests on to the Local Data Officer for attention at school level.

11. Parental requests to see the educational record

- 11.1 For Academies there is no automatic parental right of access to the educational record within a school.
- 11.2 However, within our Academy Trust we would direct parents to the school's Local Data Officer for such requests in the first instance.

12. Biometric recognition systems

- 12.1 Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to debit their catering accounts instead of paying with cash at the tills), we will comply with the requirements of the [Protection of Freedoms Act 2012](#). Please note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.
- 12.2 The Trust maintains a Biometric Policy to set out the use of Biometric Data in all PKAT Schools.
- 12.3 Any queries regarding Biometric Data and its uses that are not addressed in the Trust's Policy can be directed to the school's main office in the first instance.

13. CCTV

- 13.1 We use CCTV in various locations around each school's site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.
- 13.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
- 13.3 Any enquiries about the CCTV systems should be in the first instance be directed to the school's Main Office in the first instance.

14. Photographs and videos

- 14.1 As part of our everyday activities, we may take photographs and record images of individuals within our Academy Trust's schools.
- 14.2 Where a student is under the age of 18, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where a student is over the age of 18, we will ask for consent from the student.
- 14.3 Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.
- 14.4 Schools within our Academy Trust and the Trust itself may use photographs, images and videos for the following non-exhaustive list of instances:
 - (a) Within a school on notice boards and in school magazines, brochures, newsletters, etc.
 - (b) Outside of a school by external agencies such as the school photographer, newspapers, campaigns
 - (c) Online on our school website or social media pages
 - (d) Within Trust publications or media outputs
- 14.5 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
- 14.6 When using photographs and videos in this way we will not accompany them with any other personal information about the child.

- 14.7 See our Trust Child Protection and Safeguarding Policies and Code of Conduct for more information on our use of photographs and videos.

15. Data protection by design and default

- 15.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- (a) Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
 - (b) Identifying Local Data Officers to support compliance at school level
 - (c) Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
 - (d) Completing privacy impact assessments where the Academy Trust or member school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO can advise on this process)
 - (e) Integrating data protection into internal documents including this policy, any related policies and privacy notices
 - (f) Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
 - (g) Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
 - (h) Maintaining records of our processing activities, including:
 - (i) For the benefit of data subjects, making available the name and contact details of each school's Local Data Officer and the Academy Trust's overall DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - (ii) For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

16. Data security and storage of records

16.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

16.2 In particular:

- (a) Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept securely when not in use
- (b) Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- (c) Where personal information needs to be taken off site, staff must take personal responsibility for the safe and secure storage of the information
- (d) Passwords for electronic devices shall be subject to criteria that give them appropriate complexity and therefore strength.
- (e) Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. The use of removable media will be discouraged.
- (f) Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [eSafety and Acceptable Use Policy](#))
- (g) Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of records

17.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

17.2 For example, we will ensure the shredding, incineration or disposal of secure paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy Trust or member school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data incidents

- 18.1 The school will make all reasonable endeavours to ensure that there are no personal data incidents.
- 18.2 In the event of a suspected data incident, we will follow the procedure set out in appendix 1.
- 18.3 When appropriate, we will report a data incident to the ICO within 72 hours. Such incidents in a school context may include, but are not limited to:
- (a) A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
 - (b) Safeguarding information being made available to an unauthorised person
 - (c) The theft of a school laptop containing non-encrypted personal data about pupils
 - (d) Loss of information or equipment containing information relating to data subjects
- 18.4 An Incident Management Plan must be completed in conjunction with the process taking place regarding containing and dealing with a suspected or confirmed incident. This can be found at Appendix 2.

19. Training

- 19.1 All staff and governors are to be provided with data protection training as part of their induction process.
- 19.2 Local Data Officers will receive specific GDPR training upon appointment to enable them to effectively support the upholding of this policy and to respond to the DPO, and their audit process, in an efficient and expedient manner.
- 19.3 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

- 20.1 The COO supported by the DPO is responsible for monitoring and reviewing this policy. The Local Data Officers are obliged to keep up to date with appropriate legislation and developments around data protection matters and

share information they receive as appropriate to ensure the policy remains up to date and fit for purpose.

- 20.2 This policy will be reviewed **every 2 years** in-line with information in the [Department for Education's advice on statutory policies](#) and shared with the Board of Trustees.

21. Links with other policies

- 21.1 This data protection policy is linked to various policies at both Academy Trust and school level including but not limited to:
- (a) Freedom of information publication scheme
 - (b) Privacy Notices
 - (c) eSafety and Acceptable Usage Policy
 - (d) Child Protection and Safeguarding Policy
 - (e) Code of Conduct for All Adults
 - (f) Biometric Data Policy

22. Version History

22.1 Table of Versions

VERSION	ACTION	RESPONSIBLE	DATE
1.0	Policy drafted	Matthew DEERE	24/04/2018
1.1	Policy amended considering CEO commentary	Matthew DEERE	06/06/2018
1.2	Policy amended following feedback from all Trust schools	Matthew DEERE	02/07/2018
1.3	'Data incident' preferred to 'data breach' on LA advice	Matthew DEERE	03/07/2018

1.4	Minor changes arising from Trust Board Meeting implemented and policy approved	Matthew DEERE	08/08/2018
2.0	Regular scheduled review to include LDO and DPO input	Matthew DEERE	01/04/2020
2.1	Added further links to Biometric Data Policy and clarity to point 14.2	Matthew DEERE	23/06/2020
3.0	Interim update clarifying clauses: 10.1(b) and 10.1(c)	Matthew DEERE	04/11/2020
3.1	Branding updated and bi-annual review with GDPR Sentry	Matthew DEERE	23/05/2022

APPENDIX 1 - PERSONAL DATA INCIDENT PROCEDURE

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a data incident, or potential data incident, the staff member or data processor must immediately notify the school's Headteacher and Local Data Officer (LDO). The LDO should then inform the Trust DPO.
- It will be determined, normally by the Headteacher in conjunction with their Local Data Officer, whether a data incident has occurred. To decide, it will be considered whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The Headteacher may alert the Chair of the Local Governing Body, and in serious instances the Chief Executive Officer may be notified and share with the Chair of the Board of Trustees.
- The initial local response to a confirmed incident will be that all reasonable efforts will be made to contain and minimise the impact of the incident, ordinarily by the Local Data Officer assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- A record of the incident should be compiled on GDPR Sentry. Instructions how to do this are within Appendix 3.
- Notes of the management actions surrounding the data incident should be kept. A template for this can be found at Appendix 2. Its primary purpose is to record containment measures and initial responses. Please note such records may form part of an investigatory process and evidence bundle if there is a possible misconduct case to answer.
- The Local Data Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Headteacher will work out whether the incident must be reported to the ICO using information provided by the Local Data Officer and that which has been included in the Incident Management Plan. The Headteacher may consult with the DPO where appropriate. This must be judged on a case-by-case basis. To decide, the Headteacher will consider whether the incident is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation

- Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO or Local Data Officer must support the Headteacher to notify the ICO.
 - The decision will be documented (either way), in case it is challenged at a later date by the ICO or an individual affected by the incident. This should be within the Incident Management Plan record.
 - Where the ICO must be notified, the Headteacher or Local Data Officer must communicate with the DPO and the DPO will report via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the colleague reporting will set out:
 - A description of the nature of the personal data incident including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO and/or Local Data Officer
 - A description of the likely consequences of the personal data incident
 - A description of the measures that have been, or will be taken, to deal with the incident and mitigate any possible adverse effects on the individual(s) concerned
 - If all the above details are not yet known, the reporting officer will input as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the reporting officer expects to have further information. The reporting officer will submit the remaining information as soon as possible.
 - The reporting officer will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the reporting officer will promptly arrange for the informing, in writing, all individuals whose personal data has been compromised. This notification will set out:
 - The name and contact details of the DPO and Local Data Officer / school Headteacher
 - A description of the likely consequences of the personal data incident
 - A description of the measures that have been, or will be, taken to deal with the data incident and mitigate any possible adverse effects on the individual(s) concerned
 - The reporting officer will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
 - The Trust will keep record of each incident occurring within the Trust or any of its schools, irrespective of whether it is reported to the ICO. For each incident, this record will be made on GDPR Sentry and will include information from the Incident Management Plan:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
 - A meeting will be convened to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible and may include the Headteacher, Local Data Officer, DPO, Chair of Local Governing Body, ICT professional, Business Manager, Chief Executive

Officer and Chief Operating Officer dependent on the nature, scale, and impact of the incident, and containment thereof.

Actions to minimise the impact of data incidents

We will take actions to mitigate the impact of different types of data incident, focusing especially on incidents involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data incident.

APPENDIX 2 - INCIDENT MANAGEMENT PLAN TEMPLATE

- This should be read alongside the ICO Guidance on Data Security Breach Management
- Records of any actions taken should be attached to this form

Summary of Incident

What happened?

When did the school / the Academy Trust become aware of the incident?

Containment and Recovery

Who will be responsible for investigating the incident and taking any required action?

Does anyone else within the school / the Academy Trust need to be made aware of the incident?

Actions identified

Date action completed

Assessment of Risk

Assessment

a) will the incident cause adverse consequences to any individual?

b) how many individuals are involved?

c) who are the individuals?

d) how serious are the potential consequences - could any harm come to the individuals?

e) what data was involved in the incident?

f) how sensitive is the data?

g) are there any protections in place for the data (e.g. encryption)?

h) what has happened to the data?

i) is there any risk to the public?

Level of risk identified

Low		Medium		High	
-----	--	--------	--	------	--

Notification of Incident

Should the individual be notified (give reasons for the decision)?

Should the ICO be notified (give reasons for the decision)?

Should anyone else be notified - e.g. banks, the police (give reasons for the decision)?

Has the Trust DPO been notified of the incident, regardless of the ICO notification decision?

Is there a record created on GDPR Sentry? Note the reference number, time and date of record creation:

Evaluation and Response

Why did the data incident happen?

Are there any steps that the school should take in response to this particular incident, or to strengthen its data protection practices generally?

Please give details of a meeting convening, if appropriate, to evaluate the data incident, its management, and the preventative measures implemented to avoid future occurrences.

Signed:

Date:

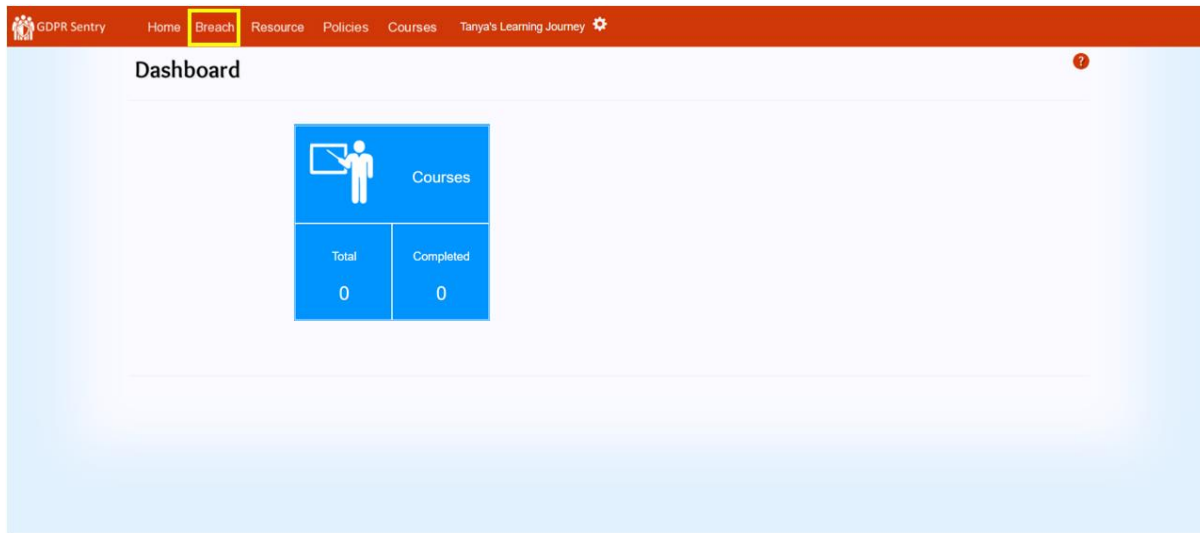
Position:

School:

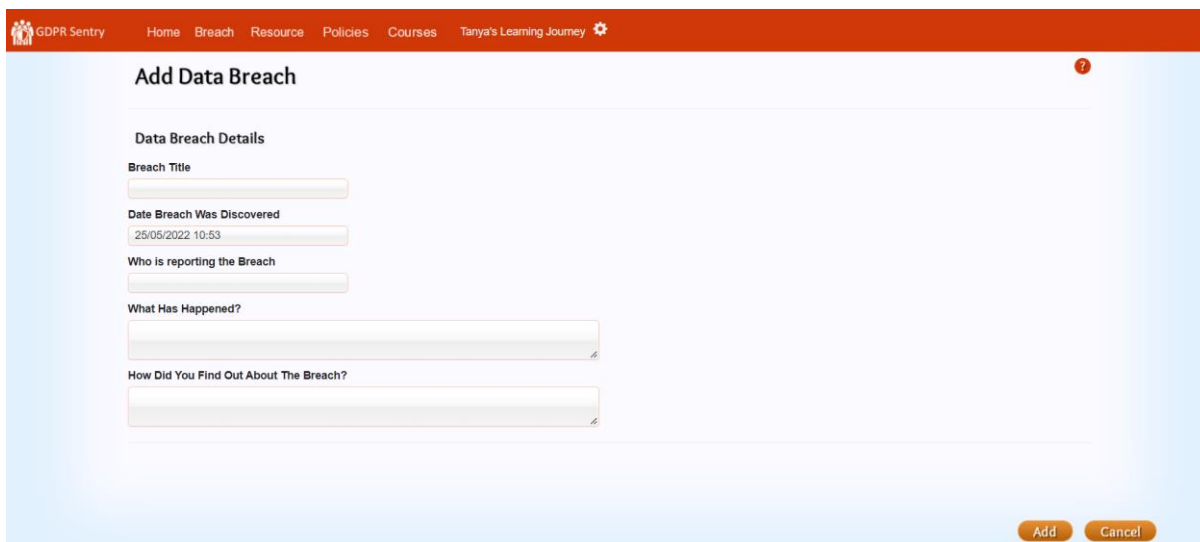
APPENDIX 3 - Recording a Data Incident

Recording a data incident as a limited user:

Limited users cannot see records held in the sentry system, but can report a data incident. To do this, click the incident button at the top of the Sentry system page.



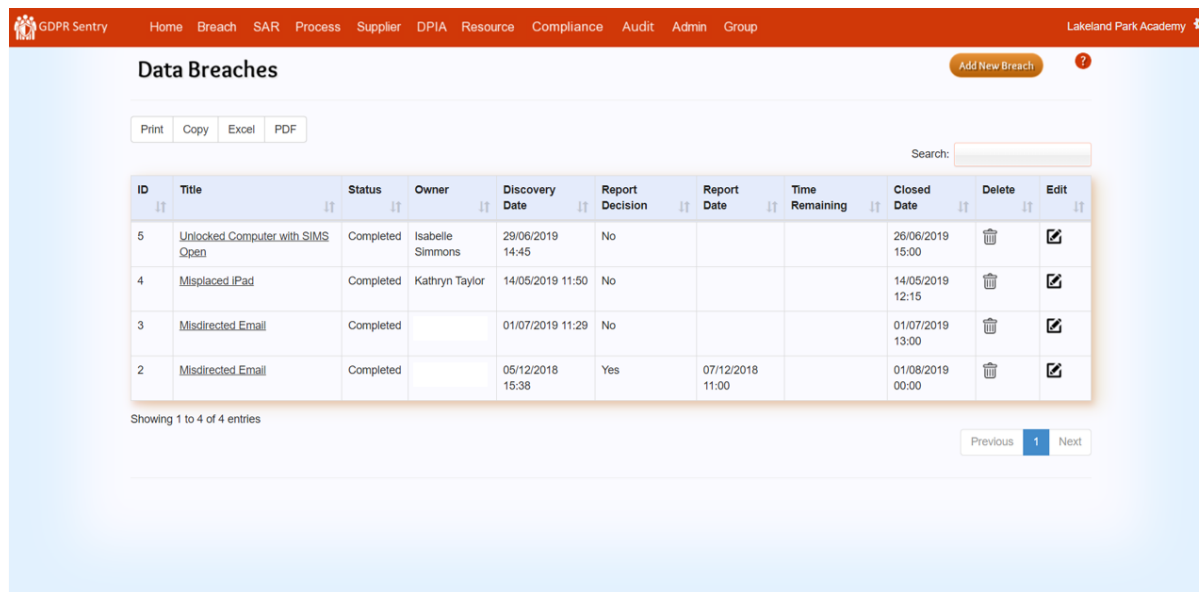
Click on this button, and you can add a data incident to the system. You can answer a few simple questions, such as when the incident was discovered, and what has happened. Answer in as much detail as you can. The more detail you provide now, the easier it will be to investigate the incident.

A screenshot of the 'Add Data Breach' form in the GDPR Sentry web application. The top navigation bar is orange and contains the following items: 'GDPR Sentry' (with a logo), 'Home', 'Breach', 'Resource', 'Policies', 'Courses', and 'Tanya's Learning Journey' (with a gear icon). Below the navigation bar, the page title is 'Add Data Breach'. The form is titled 'Data Breach Details' and contains the following fields: 'Breach Title' (text input), 'Date Breach Was Discovered' (text input with the value '25/05/2022 10:53'), 'Who is reporting the Breach' (text input), 'What Has Happened?' (text area), and 'How Did You Find Out About The Breach?' (text area). At the bottom right of the form, there are two buttons: 'Add' and 'Cancel'.

Once done, click the add button in the bottom right hand corner. This will add the incident as a record, and will send a notification to the GDPR lead for that Sentry system.

Recording a data incident as a Standard User (and above):

First click the incident button at the top of the dashboard page (or click the large orange incident tile). This will take you to a page showing all the data incidents recorded on the system (or any incidents you have the access level to view)



The screenshot shows the 'Data Breaches' page in the GDPR Sentry system. The page has a navigation bar at the top with links for Home, Breach, SAR, Process, Supplier, DPIA, Resource, Compliance, Audit, Admin, and Group. The user is logged in as 'Lakeland Park Academy'. The main content area displays a table of incidents with the following data:

ID	Title	Status	Owner	Discovery Date	Report Decision	Report Date	Time Remaining	Closed Date	Delete	Edit
5	Unlocked Computer with SIMS Open	Completed	Isabelle Simmons	29/06/2019 14:45	No			26/06/2019 15:00		
4	Misplaced iPad	Completed	Kathryn Taylor	14/05/2019 11:50	No			14/05/2019 12:15		
3	Misdirected Email	Completed		01/07/2019 11:29	No			01/07/2019 13:00		
2	Misdirected Email	Completed		05/12/2018 15:38	Yes	07/12/2018 11:00		01/08/2019 00:00		

Below the table, it says 'Showing 1 to 4 of 4 entries' and there are 'Previous', '1', and 'Next' navigation buttons.

To add a incident, click the “Add new Incident” button in the top right corner.

The status page:

Here you should add the title of the incident, and key information such as when the incident occurred and when it was discovered. If the incident is sensitive, you can restrict access to specified users on this page (remember to add yourself as a specified user.)

Details:

Here you should write a record of how the incident has occurred. Try to write in full sentences, and add as much detail as possible. This it easier to report incident to the ICO, should it be necessary.

Cyber:

While most incidents are caused by human error, if a incident has occurred due to a cyber-security issue, such as a ransomware attack or phishing scam, this should be recorded here.

Actions:

You should record here any actions taken to mitigate damage caused by this incident. This should include both actions taken to stop incidented information from spreading any further, as well as actions to prevent a similar incident occurring in the future. Similarly to the details page, this should be recorded in full sentences with as much detail as possible.

Validity:

On this page you assess whether the incident is valid or not. In most cases it will be a valid incident, so the key thing to assess on this page is whether or not you will be reporting the incident to the ICO.

ICO

Here you should state whether the incident has been reported to the ICO, and if so, when the incident was reported. You should select the reason for reporting to the ICO. It may be you believe the incident is severe enough to report to the ICO, or it may be that you are unsure, and are reporting to err on the side of caution. You should select the option that applies.

Report:

Click the “Report Export” button to download a copy of the ICO report. This should be checked over, and then sent to GDPR Sentry as a final version. GDPR Sentry will then communicate with the ICO on your behalf.