SYNERGY EDUCATION TRUST

Data Protection Policy

Inc data breach and subject access request

Current version/Level:	V2
Created by:	Lisa Tupman (in partnership with DPO Blackpool Council)
Created on:	16.04.2024 Updated 14.01.25
Next Review Date:	June 2026
Previous review dates:	NA
Adopted by Trustees on:	26.11.2024

This policy refers to the 'Trust' throughout. This incorporates the Synergy Education Trust central team and all schools who form part of the Trust.

Introduction

Synergy Education Trust collects, holds and processes personal data about pupils, staff, parents/carers, governors, visitors and other individuals who have contact with the Trust. It has a number of legal obligations under the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

Synergy Education Trust and its academies are defined as data controllers, as they 'determine the purpose and means of processing of personal data' and as such pay an annual fee to Information Commissioner's Office as required by the Data Protection (Charges and Information) Regulations 2018.

This policy commits that the Trust will also comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, the Protection of Freedoms Act 2012 when referring to use of biometric data and Article 8 of the Human Rights Act 1998.

Scope

This policy applies to all personal data held as information in any format including paper, electronic, images and sound, and emails that may be sent or received by the Trust.

All stages of the lifecycle of personal data are covered by this policy:

- Obtaining of data;
- Storage and security of data and any information this data creates;
- Use and disclosure of data and any information this data creates;
- Sharing of data and any information this data creates;
- Disposal and destruction of data and any information this data creates.

This policy applies to all part-time and full-time employees, including those working from home and from other locations and all other workers (including casual and agency workers, secondment posts and contractors) using the Trust's equipment and computer network. This policy also applies to volunteers and students (including work experience or work-placement).

Definitions

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The UK GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

Data Protection Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

a. Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...] ('purpose limitation').
c. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are process ('data minimisation').
d. Accurate and, where necessary, kept up to date; every reasonable step to ensure inaccurate data are erased or rectified without undue delay ('accuracy').
e. Kept in a form which permits identification of the individual for no longer than is necessary for the purpose which the data are processed [...] ('storage limitations').
f. 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 ('integrity and confidentiality').

Lawful Processing

The Trust will only process personal data if one of the following conditions are met, which are outlined in Article (6)(1) of the UK GDPR:

- Data subject has given consent to the processing of their personal data. This consent will be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. Consent will be recorded and once withdrawn by the data subject, the Trust will cease processing data for the specified purpose without undue delay.
- Processing is necessary for the performance of a contract to which the data subject are a party to, or in order to take steps at the request of the data subject prior to entering the contract.
- Processing is necessary for compliance with a legal obligation to which the Trust is subject to.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- 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 purposes of the legitimate interests pursued by the Trust or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The Trust will only collect and process 'special categories of personal data' if one of the additional conditions set out in Article 9(2) has been satisfied.

Consent

In all cases, consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The Trust is therefore committed to obtaining consent in the following manner:

- Consent is presented in a manner clearly distinguishable from other matters.
- The request is made in an intelligible and easily accessible form using plain language.
- Is freely given (i.e. not based on the need to conduct another processing activity).
- The date, method, validity and content of the consent is documented.
- A simple method is provided for the data subject to be able to withdraw consent at any time.

Once consent is withdrawn by the data subject, the Trust will cease processing data for the specified purpose without undue delay.

If the Trust wishes to offer information Society Services (ISS) to pupils it will gain parental consent for any pupil below the age of 13.

Accountability and Governance

Data Protection Officer (DPO)

Under the UK GDPR, it is mandatory for Trusts to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- To monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- To be the first point of contact for the Information Commissioner's Office.

The contact details for the Trust's designated DPO are as follows:

Data Protection Officer, Information Governance Team
Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
TrustsDPO@blackpool.gov.uk

Staff can contact the DPO if they have any queries about this policy, data protection law, data retention or the security of personal data. The DPO can also be contacted directly if members of staff have any concerns that this policy is not being adhered to.

Record of Processing Activities (ROPA)

The Trust is required to maintain records of activities related to higher risk processing of personal data. The Trust maintains a ROPA in conjunction with their DPO. All employees are required to notify their data protection lead or DPO before they embark on any new processing activities so they can be adequately recorded on the Trust's ROPA.

Workforce Training

The Trust is committed to providing data protection training to all staff as part of their induction process and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law. The Trust

will retain a record of this training programme and this will be made available to the Information Commissioner's Office on request.

Data Protection Impact Assessments (DPIAs)

Data protection impact assessments (DPIAs) are a tool which can help the Trust identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The Trust will complete a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore, staff must consult the relevant persons or DPO before they embark on any new processing that could be regarded as being high risk to an individuals' interests. If required, the DPO will assist members of staff completing the Trust's DPIA template.

The Trust has a supplementary DPIA Procedure, which assists employees in understanding the purpose of a DPIA and when/how to complete one.

Contracts

Whenever a controller uses a processor, it needs to have a written contract in place. This is important so that both parties understand their responsibilities and liabilities. The Trust commits to including the following compulsory details in its contracts:

- The subject matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subject; and
- The obligations and rights of the controller.

The Trust has a supplementary Procurement Procedure, which outlines its commitment in more detail.

Individual Rights

Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. It is called 'privacy information' and the Trust will issue privacy notices in relation to pupil data, workforce data and governor data. The Trust will endeavour to issue these notices

on induction and also make them available on the Trust's website throughout the data subject's Trust life.

Right of Access

Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

'Subject access' requests can be submitted to the Trust office and should contain the name of the data subject, a correspondence address and a description of the information requested. The Trust will provide the information without delay and at the latest within one month of receipt of the request. The Trust will not apply a fee to requests unless the request is manifestly unfounded or excessive. The Trust will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the Trust's decision, the process for doing so will be clearly outlined in the response issued.

The Trust has a supplementary Subject Access Procedure, which outlines the process for receiving and responding to a request in more detail. Please see appendix 2.

Individual Rights

The UK GDPR also empowers individuals with the right to rectification, erasure, right to restrict processing, data portability, right to object and rights in relation to automated decision making or profiling. Any requests should be passed to the Trust's Data Protection Lead as soon as received, who will consider the request alongside the DPO.

Data Security

Principle f of the UK GDPR states data should be processed in a manner that ensures appropriate security of the personal data. This means that the Trust must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- Portable electronic devices, such as laptops, ipads and hard drives that contain personal data are stored in a locked cupboard or draw.
- Encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices.
- Passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons.
- Where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified.
- When sending personal data to a third party, staff must carefully check the recipient and their contact details.
- Where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device.
- Staff should not open links when emails are received from unknown recipients or the emails appear suspicious.
- Personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data.

Breach Reporting

The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, the Trust must do this within 72 hours of becoming aware of the breach. It is essential that **all members of staff make the relevant persons aware of any potential breaches of data protection without undue delay.** This includes all losses, thefts or inadvertent disclosures of personal data. It also includes the loss or theft of any device that holds personal data.

The relevant persons will then follow the breach procedure in conjunction with the DPO. An investigation will be conducted to confirm whether or not a personal data breach has occurred. If a breach has occurred the DPO will advise the Trust on whether it is required to notify the Information Commissioner and the data subjects affected. Please see appendix 1 for procedure

Data Retention

Principles of the UK GDPR states data must be 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. Data will only be retained for the specified period outlined in the records management schedule that the Trust has adopted and will be destroyed in a secure manner thereafter.

The Trust has a Records Retention Schedule which outlines its commitment to adhering to this principle and contains the Trust's model retention schedule.

Data Accuracy and Limitation

Principle d of the UK GDPR states data shall be accurate and, where necessary, kept up to date The Trust will issue regular reminders to staff and parents/carers to ensure that personal data held is up to date and accurate. Any inaccuracies discovered will be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to the individuals in the Trust's privacy notices. If the Trust wants to use personal data for reasons other than those given when it first obtains it, it will inform the individuals concerned before it does so, and seek consent where necessary. Staff must only process personal data where it is necessary to do so in their jobs.

Information Requests

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 Trust days of receipt of a written request. The Trust will adhere with 'subject access' requests as outlined in Section 7.2 of this policy.

Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

Requests for personal data by the Police or other bodies with law enforcement powers (e.g. HMRC), will usually only be considered when accompanied by an appropriate data protection exemption. The request should contain details of the applicant, the purpose of the request and the section of the legislation the information is being requested under. This will allow the DPO to make an informed decision as to whether the request is proportionate for the purpose requested, against the rights of the data subject.

If requests are received from parents/carers for the names of pupils in their class (e.g. for Christmas card or birthday invites), only first names will usually be released, however the Trust reserves the right to refuse any request in its entirety.

Surveillance and CCTV

The Trust uses CCTV in various locations around the Trust sites; as such it adheres to the ICO's code of practice for the use of CCTV. The Trust does not need to ask individuals' permission but cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system or requests for footage should be directed to the Trust office.

Appendix 1: Personal Data Breach Procedure

Introduction

The UK General Data Protection Regulation (UK GDPR) places a requirement on Trusts to have a formal process in place to manage personal data breaches.

This procedural guide describes what a personal data breach is and the process which must be followed in the event of a breach.

This guidance applies to all employees, partners, volunteers, suppliers, contractors and Governors (collectively referred to as 'users') who process, have access to, hold or who are responsible for the Trust's personal data. All users must understand and adhere to this guidance, with it applying to all personal data, regardless of whether it is held in a paper or electronic format.

Personal Data Breach Definition

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access to personal data by an unauthorised third party e.g. a cyber-attack;
- Sending personal data to an incorrect recipient e.g. email or a letter;
- Paper records containing personal data being lost or stolen;
- Electronic devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

A personal data breach is broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever;

- Any personal data is lost, destroyed, corrupted or disclosed without permission

- If someone accesses the data or passes it on without proper authorisation;

- If the data is made unavailable, for example, when it has been encrypted by ransomware, or lost or destroyed.

When a security incident takes place, the School should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

Personal Data Breach Process

Should a user discover a data breach, they must immediately report this to their respective School Data Protection Lead.

The Trust Data Protection Lead is:

Lisa Tupman, Chief Operating Officer

Synergy Education Trust, Stanley Primary School, Blackpool, FY3 9UT

admin@seteducation.org.uk

If the Data Protection Lead is unavailable it should be brought to the attention of an alternative member of the Senior Leadership Team (SLT).

The Data Protection Lead or member of SLT should immediately report the personal data breach to the Trust's Data Protection Officer (DPO) using the online https://forms.office.com/e/y3yZkzAxxR

Please see below for a hardcopy version.

The DPO will then initiate an investigation of the personal data breach and advise the School/Trust on any actions it should take to contain or recover the personal data. The DPO will conduct an assessment of the likelihood and severity of the resulting risk to the data subject's rights and freedoms. Based on this assessment the DPO will issue formal guidance to the School / Trust on whether the ICO or data subject should be notified. The DPO will work closely with the School / Trust with regards to any remedial actions to prevent a reoccurrence.

The contact details for the School / Trust designated DPO are as follows:

Data Protection Officer, Information Governance Team
Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
SchoolsDPO@blackpool.gov.uk

ICO Notification - Criteria

When a personal data breach has occurred, the DPO will undertake an assessment of the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then the DPO will advise the School / Trust that the incident is required to be referred to the ICO. However, please note that the specific ICO Breach Notification Form must only be completed and submitted by the DPO.

If it is unlikely to result in a risk to people's rights and freedoms then the School / Trust does not have to notify the ICO. However, once it is decided that the breach does not need to be reported, the decision must be justified and the reasons for that decision must be documented by the DPO.

In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals.

Recital 85 of the UK GDPR explains that:

> *'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned'.*

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job.

If a data processor contracted on behalf of the School / Trust has encountered a personal data breach, then under Article 33(2) of the UK GDPR, the data processor must inform the School / Trust without undue delay and as soon as the data processor becomes aware.

The requirements on breach reporting should always be detailed in the contract between the School / Trust and its processor. This requirement then allows School / Trust to take steps to address the breach and meet its breach-reporting obligations.

ICO Notification - Timeframes

The DPO must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If School / Trust takes longer than this, then it must give reasons to the ICO for the delay.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4) allows the organisation to provide the required information in phases, as long as this is done without undue further delay.

ICO Notification - Content

When the DPO reports a breach to the ICO, the UK GDPR states they must provide:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of your global turnover. The fine can also be combined with the ICO's other corrective powers under Article 58 of the UK GDPR.

Data Subject Notification

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says the School / Trust must inform those concerned directly and without undue delay. When a personal data breach has occurred, the DPO will conduct an assessment of the likelihood and severity of the resulting risk to people's rights and freedoms, and advise the School / Trust whether they are required to notify the data subject.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, the DPO will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this

occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, users will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If the School / Trust decide not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The School / Trust should also remember that the ICO has the power to compel them to inform affected individuals if they consider there is a high risk. In any event, the DPO should document their decision-making process in line with the requirements of the accountability principle.

Data Breach Repercussions

ICO

The ICO has the power to take action against organisations in line with Part 5 of the Network and Information Systems Regulations 2018. The regulations are primarily aimed at improving cybersecurity and relates to any 'incident' that has an impact on a service which includes 'non-cyber' causes.
The ICO have the following enforcement powers:

- Information notices
  Under Regulation 15(3), the ICO may serve an 'information notice' (IN)
  The IN will describe the information the ICO require, the reasons why it is required, how it should be provided and the time period.
- Enforcement notices
  Under Regulation 17(2), the ICO may serve an enforcement notice (EN) when they have reasonable grounds to believe an organisation have failed to:
  - fulfil their security obligations
  - notify the ICO of a security incident
  - comply with their notification obligations
  - notify the public about any incident, if it was deemed a requirement to do so
  - comply with an Information Notice
  - complying with inspection requirements
- Inspection powers

Under Regulation 16(2), the ICO has the power to conduct an inspection to see if an organisation has fulfilled their security obligations

- Penalty notices
  Regulation 18(2) gives the ICO the power to serve a penalty notice on an organisation in certain circumstances. Penalties will be issues that are appropriate and proportionate to the failure.

Right to Compensation

Under Article 82 of the UK GDPR 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'
Material damage = financial loss.
Non-material damage = the individual has suffered distress.

Employee

All members of staff have responsibility for how the School / Trust collects, holds and processes personal data. Staff found to be in breach of the Personal Data Breach Procedure, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.
Breaches of any School / Trust policies and procedures will be dealt with as a matter of conduct, capability or performance via the School / Trust's existing Human Resources policies and procedures.

Criminal Proceedings

Section 170 of the Data Protection Act 2018 states that it is a criminal offence for a person to knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller.
Examples include:

- School data being taken, retained or transferred unlawfully
- Deliberately deleting School data to prevent it being disclosed in response to a Subject Access Request (SAR)
- Re-exposing previously redacted material

The School / Trust, as a data controller has a legal responsibility to report potential offences to the ICO where an assessment will be carried out by their Criminal

Investigation Team. During their assessment, they will decide where there is sufficient evidence to support a prosecution or if it is in the public interest to prosecute.

Examples of data breaches

	• A school has apologised for sending an email to parents which listed the personal data of 69 pupils who were being disciplined for bad behaviour. • The message included an attachment which contained information about free school meal eligibility and pupils' special educational needs (SEN) status. • Made a self referral to the Information Commissioner's Office (ICO).
	• Highly confidential documents from 14 schools have been leaked online by hackers. Vice Society makes demands for money to prevent it leaking documents on the dark web • Hacking' is a process where by a 'hacker' gains unauthorised access to a system, network or computer by exploitation of its areas of weakness. • Folders accessed consisted of passport scans for pupils and parents, contractual offers, teaching documents and student bursary fund recipients.
	• The former head teacher of a school in Ashford was ordered to pay more than £1,000 after he admitted unlawfully obtaining school children's personal data. • The staff member was suspended for six months • The staff member had no lawful reason to process the data and provided "no valid explanation" for how it had appeared on the server, instead claiming they had deleted the personal data from his USB stick. • The former Headteacher appeared at Ealing Magistrates' Court and admitted two offences of unlawfully obtaining personal data and was subsequently fined.

Data Breach Form: Paper Copy

Use this Form to report a potential data breach to the School's Data Protection Officer (DPO). A form should be submitted immediately when you become aware of a potential data breach because the school must report a notifiable breach to the ICO without undue delay, but not later than **72 hours**. If this form is being submitted later please explain why.

1. What date was the incident discovered?	2. What time was the incident discovered?	3. Date the Incident Occurred	4. What time did the incident occur?

5. Police and Crime log number (if applicable)

6. Details of the Incident and An Actions Taken To Date *(include type of data, format of data e.g. electronic or physical. Has the incident been recalled / rectified / returned / deleted?)*

7. How did you find out about the incident?

8. Approximately how many people have been affected?

9. Who has been affected?	Please mark
Pupils (including former pupils)	☐
Parents / Carers / Guardians	☐
Employees	☐
Governors	☐
Other	☐

10. List the names of the people involved

11. Have you informed the data subjects that this incident occurred?	Yes	No	Not Applicable
Please mark	☐	☐	☐

12. Please provide an estimate regarding the likelihood of harm caused following this data breach	Please mark
Not Occurred	☐
Not Likely	☐
Likely	☐
Highly Likely	☐
Occurred	☐

13. Please provide an estimate regarding the impact caused following this data breach (actual and considered potential impact)	Please mark
Effect	☐
Minor	☐
Adverse	☐
Serious	☐
Catastrophic	☐

14. Is there any further information you would like to provide?

The contact details for the School / Trust designated DPO are as follows:

Data Protection Officer, Information Governance Team

Postal Address: Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
Email Address: SchoolsDPO@blackpool.gov.uk
Telephone Number: (01253) 478980

Appendix 2: Subject Access Request Procedure

Introduction

The UK General Data Protection Regulation (UK GDPR) places a requirement on the School / Trust to comply with the 'right of access' which applies to all personal data that it holds. A detailed definition of personal data is included in the Data Protection Policy.

This procedural guide describes what a subject access request is and the process which must be followed in the event of a request.

Responsibility for complying with a subject access request lies with the School / Trust as a data controller, therefore this guidance applies to its employees and processors. The School / Trust will ensure that they have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to the School / Trust or a processor. This guidance applies to all personal data, regardless of whether it is held in a paper or electronic format.

Definition

Article 15 of the UK GDPR aka the Right of Access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data and check that the School / Trust using it lawfully.

Individuals have the right to obtain the following from the School / Trust:

- Confirmation that the School / Trust are processing their personal data;
- A copy of their personal data; and
- Other supplementary information – (please see below)
    - The purposes of processing;
    - The categories of personal data concerned;
    - The recipients or categories of recipient the School / Trust disclose the personal data to;
    - The School / Trust retention period for storing the personal data
    - The existence of their right to request rectification, erasure or restriction or to object to such processing;

- The right to lodge a complaint with the ICO or another supervisory authority;
- Information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and
- The safeguards the School / Trust provide if they transfer personal data to a third country or international organisation.

The School / Trust provides much of this information already in its Pupil Privacy Notice and Employee Privacy Notice.

Process

The UK GDPR does not specify how to make a valid request and a request does not have to include the phrase 'subject access request' or Article 15 of the UK GDPR, as long as it is clear that the individual is asking for their own personal data. – please see *section 5* for more details how this relates to parents requesting their child's records.

Therefore, an individual can make a subject access request verbally or in writing. It can also be made to any individual who is connected to the School / Trust (including by social media) and does not have to be to a specific person or contact point.

However, a standard form can make it easier both for the School / Trust to recognise a subject access request and for the individual to include all the details required to locate the information they want. A copy of the standard form is available in Appendix A and if willing, applicants should be directed to use this form in the first instance.

If an employee receives a subject access request, they must immediately direct it to the Data Protection Lead.

The Trust Data Protection Lead is:

Lisa Tupman, Chief Operating Officer

Synergy Education Trust, Stanley Primary School, Blackpool, FY3 9UT

admin@seteducation.org.uk

If the Data Protection Lead is unavailable it should be brought to the attention of a member of the Senior Leadership Team (SLT).

The Data Protection Lead or member of SLT should immediately seek the advice of the School / Trust designated Data Protection Officer (DPO).

The contact details for the School / Trust designated DPO are as follows:

Data Protection Officer, Information Governance Team
Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
SchoolsDPO@blackpool.gov.uk

If the School / Trust has doubts about the identity of the person making the request they will ask for more information. If this is the case the School / Trust will let the individual know as soon as possible that they need more information from them to confirm their identity before responding to their request.

Timeframe

The School / Trust must act on the subject access request without undue delay and at the latest within one month of receipt. This must be no later than one calendar month, starting from the day the request is received. If the School / Trust needs something further to be able to deal with the request (such as ID documents), the time limit will begin once they have received this.

The School / Trust can extend the time to respond by up to a further two months if the request is complex or they have received a number of requests from the individual. The School / Trust should let the individual know within the one month of receiving their request and explain why the extension is necessary. The request is complex generally if there is large amounts of data to be extracted and collated from a number of different systems and redactions to be applied. Whether a case is deemed complex is determined on a case-by-case basis by discussion with the DPO Service and applying the specific ICO criteria to the request.

Requests Made by Parents / Guardians / Carers

Before responding to a subject access request for information held about a pupil, the School / Trust should consider whether the child is mature enough to understand their rights. This is usually at around the age of 12 or over. If we are confident that the child can understand their rights, then we will usually respond directly to the child. The School / Trust may however allow the requester to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

The child should able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the School / Trust (with DPO advice) will take into account, amongst other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents/guardian should have access to information about them.

The School in partnership with the DPO will seek the advice of appropriate professionals when considering the above factors

Requests made on Behalf of or by Others

The UK GDPR does not prevent an individual/parent making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, the School / Trust will need to be satisfied that the third party making the request is entitled to act on behalf of the parent or individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Exemptions

In some circumstances, the Data Protection Act 2018 (DPA 2018) provides an exemption from particular UK GDPR provisions. If an exemption applies, the School / Trust may not have to comply with all the usual rights and obligations. There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.

Common examples of exemptions fall in the following categories:

- Prevention & Protection of Crime.
- Legal Professional Privilege or Court documentation

- Protection of the Rights of Others.
- Health, social work, education and child abuse data.

The DPO will advise on the application of any exemptions with redactions being kept to a minimum and the context of information retained where possible. The exemptions applied will also clearly be outlined in the response letter issued in response to any request.

Disclosures

In most cases, School / Trust cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive the School / Trust may charge a 'reasonable fee' for the administrative costs of complying with the request. School / Trust can also charge a reasonable fee if an individual requests further copies of their data following a request.

The School / Trust will include an individual's right to appeal decision in all response letters, in the first instance this will be an internal review of any decision and then if the applicant is still dissatisfied they can appeal directly to the ICO.

Subject Access Request Form

Name of applicant	
Date of birth	
Address	
Description of the information	

Name of requestor *(if not data subject)* and any authority held	

Date: **********

Name
Address Line 1
Address Line 2
Address Line 3

Our Ref: 00000/D1
Your Ref: 00000
Direct Line: 00000
Email:********

Dear **********

Data Protection Act 2018 and the UK GDPR – Subject Access Request

Thank you for your request for personal information that was received by the School/Trust on insert date.

You have submitted a request for:

- insert here what they have asked for e.g. a copy of your child's education records.

This will be dealt with under Article 15 of the UK GDPR. This places on obligation upon the School/Trust to reply as promptly as possible but within one calendar month. This time period can be extended by another two calendar months if the request is complex.

If appropriate or need to verify identity/address please use this paragraph:

To ensure that we provide the correct information to the correct person we will require proof of identity and address of each person/child. Pending receipt of these, we will conduct a search for the records you have requested.

The School/Trust has an obligation to protect the identity of others (third parties) unless they have given their consent for disclosure, or it is appropriate to disclose. Therefore, you are advised that some information may be withheld and if this applies, you will be informed at the time of disclosure.

If you have any queries please do not hesitate to contact me on the number or email address above.

Yours sincerely

XXXXXXXXXXXXX

Extension letter

Date: **********

Name
Address Line 1
Address Line 2
Address Line 3

Our Ref: 00000/D3
Your Ref: 00000
Direct Line: 00000
Email: **********

Dear **********

Data Protection Act 2018 and the UK GDPR – Subject Access Request;

Thank you for your request for personal information that was received by the School/Trust on insert date.

You have submitted a request for:

- insert here what they have asked for e.g. a copy of your child's education records.

This will be dealt with under Article 15 of the GDPR. This places on obligation upon the School/Trust to reply as promptly as possible but usually no later than within one month of receipt; however, we can in certain circumstances extend this timescale under the regulation.

If appropriate or need to verify identity/address please use this paragraph:

To ensure that we provide the correct information to the correct person we will require proof of identity and address of each person/child. Pending receipt of these, we will conduct a search for the records you have requested

I can confirm that after careful consideration we will unfortunately need to extend the timescale in which we are able to respond to your request by an additional two months. This is because we deem the request to be complex. We have considered your request against the complex request criteria as specified in the Information Commissioner Guidance on the UK GDPR's Rights of Access – the criteria used for your request is stated below;

- The Trust/School will be required to collate a large volume of information both electronic and paper.

In addition to this and to satisfy the criteria for the extension; please pick at least one – can add individual description as per the case.

- The request requires the School to retrieve a large amount of historical information, some of which is contained within several electronic and/or paper recording systems for information such as emails/first aid records.
- There has been/will be technical difficulties in retrieving the information – add reason i.e. archived on old systems
- The Trust/School has applied an exemption that involves large volumes of particularly sensitive information
- The Trust/School has had to/will have to clarify potential issues around disclosing information about a child to a legal guardian
- Any specialist work involved in redacting information or communicating in an intelligible format

Therefore, a response will be issued no later than: xxxxxxxxxx. If you have any queries about this letter, you can contact us by email at: xxxxxxxxxxxxxxxxxxxx

.

Yours sincerely

****

Redacted response letter

Date: *********

Name
Address Line 1
Address Line 2
Address Line 3

Our Ref: 00000/D2
Your Ref: 00000
Direct Line: 00000
Email: **********

Dear **********

Data Protection Act 2018 and the UK GDPR – Subject Access Request

Thank you for your request for personal information that was received by the School/Trust on insert date.

You submitted a request for:

- insert here what they have asked for e.g. a copy of your child's education records.

The information is enclosed/attached. You will notice that there have been some redactions made (blacking out). This is because the following exemptions apply:
Insert exemptions – DPO will provide a list of these.
The School/Trust processes this personal data for the primary purpose of provision of Education. For more information on this please see our Privacy Notice, which can be found on our website – provide link.
Under the UK GDPR, you have a number of rights, including the right to have any incorrect data rectified or erased, or the right to restrict or object to processing. We publish information about these rights on our website at provide link.
If you are dissatisfied with the handling of your request, you have a right to submit a complaint or request a review. You should submit this in writing to Data Protection Officer ********** or by email to **********.
If you are not happy with the outcome of our review, you have the right to apply to the Information Commissioner's Office (ICO) for an assessment. You can contact the ICO at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, (www.ico.org.uk).
If you have any queries about this letter you can contact me by writing to: **********.

Yours sincerely

XXXXXXXXXXXX
XXXXXXXXXXXX