Data Protection Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
V1	ADA	Data Protection Act	Trust Board	Oct 2019	March 2021
V2	RGR	New template; change GDPR to UK-GDPR; update DPL/DPO responsibilities	Trust Board	Mar 2021	Mar 2022
V3	RGR	Annual Review	Trust Board	Mar 2022	Mar 2023
V4	RGR	Update 2. Legal framework; 4. Accountability; 6. Personal data; 12. Surveillance; 27. Data Protection Officer. New: 14. Safeguarding; 15. Cloud Computing; 16. DBS data; Appendix 1.	Trust Board	Mar 2023	Mar 2024
V5	RGR	Update 4. Accountability; 20. Information Sharing.	Trust Board	Mar 2024	Mar 2025
V6	RGR	Information re US-UK data bridge.	Trust Board	Mar 2025	Mar 2026
V7	RGR	Information re Data Access & Use Act 2025 and new guidance on SARs	Trust Board	Nov 2025	Nov 2026

Contents

1. INTRODUCTION

This policy sets out how each Academy will comply with data protection legislation and protect the personal information of everyone who receives services from, or provides services to, each Academy. It informs every one of their rights, and suppliers of their responsibilities. It shows how each Academy complies with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, UK-GDPR, and other regulations and good practice standards.

2. LEGAL FRAMEWORK – UK/EU GDPR

The EU GDPR will not apply directly to UK organisations. However, all UK organisations will follow its rules which were adopted into UK law by the UK Data Protection Act (DPA) 2018. In addition, the UK government has introduced legislation, the **Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019** which amends the DPA, merging it with the requirements of the EU GDPR; this produces what has been referred to as '**UK GDPR'**. There may be some temporary changes to the rules on transfers of personal data between the UK and the EU/EEA.

This policy has regard to:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- Data Access & Use Act 2025

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

This policy operates in conjunction with the following school policies:

- Data and Cyber-security Breach Prevention and Management Plan
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- CCTV Policy
- Child Protection and Safeguarding Policy
- Records Management Policy
- Subject Access Request Policy
- E-Safety Policy
- Artificial Intelligence Policy
- Confidentiality Policy

Sharing Data

The Trust will only transfer personal data outside the United Kingdom (UK) and European Economic Area (EEA) where adequate safeguards are in place to protect the rights and freedoms of data subjects in accordance with the UK GDPR and the Data Protection Act 2018.

Personal data will only be transferred internationally where one or more of the following apply:

- The country has been granted an adequacy decision by the UK Government confirming that it provides an equivalent level of data protection.

- The transfer is covered by appropriate safeguards, such as the use of the International Data Transfer Agreement (IDTA) or EU Standard Contractual Clauses (SCCs) as recognised under UK law.
- The transfer is necessary for a specific purpose permitted under Article 49 of the UK GDPR, such as obtaining explicit consent from the data subject, performing a contract, or protecting vital interests.

Before any transfer takes place, the school's Data Protection Officer (DPO) will carry out a Transfer Risk Assessment (TRA) or equivalent due diligence to ensure that personal data remains protected.
The school will ensure that all international data sharing agreements are documented and that data subjects are informed through the Privacy Notice of any potential transfers of their personal data outside the UK or EEA.

3. SCOPE

This policy applies to parents, students, employees, contractors, trustees and school governors. It covers personal data we collect and use on paper and electronically. It covers our databases, cloud services, computer network and archive of paper records. It covers video and photographs, voice recordings, CCTV and mobile devices such as laptops, mobile phones and memory sticks.

4. ACCOUNTABILITY

Each Academy is a data controller which means that it decides why and how personal data is processed. It is accountable for its handling of personal information. Our Headteachers/Principals and Academy Governing Bodies' are accountable for providing the policies for employees to follow under the law, so that we can carry out our statutory functions. The Data Protection Policy is part of our governance framework, which contains important policies and procedures maintained and published by each Academy, that are key to good governance and effective decision making. The Senior Information Risk Officer (SIRO) is the Headteacher/Principal who is accountable for protecting the academy's information assets.

The Data Protection Officer is a position required in law to ensure our academies all comply with data protection legislation and acts as a single point of contact for individuals who want to find out about their data.

Each employee, governor and supplier is bound by a contractual duty of confidentiality.

Leger Education Trust is the overall data controller for the academies in the Trust and the registration number is available through the Information Commissioner's Office public register:
https://ico.org.uk/ESDWebPages/Entry/Z3570404

Each Academy is registered with the Information Commissioner, who is the independent regulator appointed by parliament to check compliance with data protection law.

Each Academy maintains a register of processing activities of the personal information we are responsible for to ensure it is used according to the data protection principles.

Leger Education Trust will take organisational steps to keep personal data secure, and the deployment of staff data protection training is key to reducing the likelihood of data losses. Academies will ensure that new starters will receive data protection training, proportionate to their role, before they have access to personal data and existing staff will receive regular and refresher training.

5. DATA PROTECTION IS A FUNDAMENTAL RIGHT

The protection of a person's data is a fundamental right. Under the Human Rights Act 1998, everyone has the right to respect for their private and family life, their home and their correspondence. This includes respect for your private and confidential information, particularly when storing and sharing data.

This right can be limited in certain circumstances but any limitation must balance the competing interests of an individual and of the community as a whole.

In particular, any limitation must be covered by law and be necessary and proportionate for one or more of the following aims:

- public safety or the country's economic wellbeing
- prevention of disorder or crime
- protecting health or morals
- protecting other people's rights and freedoms
- national security.

The right to privacy must often be balanced against the right to free expression. Public figures don't necessarily enjoy the same privacy as others. For example, sometimes the public interest might justify publishing information about senior officers or governors that would otherwise interfere with their right to privacy.

6. PERSONAL DATA

In this policy we use the terms "personal data" and "special categories of personal data" which are used in data protection legislation.

In this policy personal data means any information relating to an identifiable living person. This means they can be identified from information such as a name, an address, an identification number (e.g. your National Insurance number, unique pupil reference number), location data, etc.

"Special categories of personal data" is personal sensitive data. This is data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

There are extra safeguards for special categories of personal data to ensure no one is discriminated against when it comes to receiving a service.

As the Trust collates and processes data of individuals under the age of 13, additional safeguards are made in the confidentiality of their information.

We generally refer to a person or individual in this policy, although the term in law is "data subject".

The frequent reference in this policy to "processing" data means any operation performed on personal data, whether using a computer or manual filing systems. It includes collection, use, and recording, storing, sending and deleting personal data.

7. DATA PROTECTION PRINCIPLES

Each Academy applies data protection principles in its processing of personal data. These principles are set out in the General Data Protection Regulation and have been incorporated into the Data Protection Act 2018. The six principles are that personal data should be:

- Processed lawfully, fairly and in a transparent way
- Collected for a specific purpose
- Adequate, relevant and limited to what's necessary
- Kept up to date
- Kept for only as long as necessary
- Protected with appropriate security

8. LAWFUL BASIS OF PROCESSING PERSONAL DATA

There are different lawful reasons for processing personal data and special categories of personal data. The Academies always uses at least one lawful basis for processing personal information and at least one lawful basis for processing special categories of personal data.

The six lawful reasons for processing personal data are:

1- An individual has given consent for the processing of his or her personal data, and it is freely given, specific, informed, and there must be an indication signifying agreement;

2- The Academy has a contract with a person and need to process their personal data to comply with our obligations under the contract; or we haven't yet got a contract with the person, but they have asked us to do something as a first step (e.g. provide a quote) and we need to process their personal data to do what they ask;

3- The Academy is obliged to process personal data to comply with the law. We will always refer to the specific legal provision or source of advice that explains generally applicable legal obligations;

4- An academy may process personal data without consent where it meets a recognised legitimate interest, such as safeguarding, preventing crime, or responding to an emergency.

5- The processing of personal data is necessary under public functions and powers set out in law; or the council needs to perform a specific task in the public interest that is set out in law;

6- The processing of personal data is in the legitimate interests of the Academy, where we use data in ways that people would reasonably expect and that have a minimal privacy impact. However, public authorities are more limited than private organisations in their ability to rely on this basis for processing personal data;

7- Personal data may be use for additional purposes that are compatible with the original reason for collection, without the need to seek new consent, where appropriate safeguards are in place;

8- Consent remains essential when processing special category data or when automated decisions could have a significant effect on an individual

The lawful bases for processing special categories of data are:

- an individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the school or a person under employment, social security and social protection law or a collective agreement under law;
- processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent;
- processing by non-for-profit bodies for legitimate activities with appropriate safeguards;
- processing relates to personal data which have been made public by a person;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest under law;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

Each Academy must always demonstrate it processes information with safeguards in place to protect the fundamental rights and interests of the individual.

9. CONSENT

Where the Academy relies on consent or explicit consent as the lawful basis for processing, we will do this to by offering individuals real choice and control.

- We will avoid making consent to processing a precondition of a service.
- We will be clear and concise.
- We keep our requests for consent separate from other terms and conditions.
- We will be specific and 'granular' so that we get separate consent for separate things.
- We will name any third parties (i.e. other groups or organisations) who will rely on the consent.
- We will make it easy for people to withdraw consent and tell them how.
- We will keep evidence of consent (who, when, how, and what we told people).
- We will keep consent under review, and update it if anything changes.

For explicit consent we will ensure the individual provides a very clear and specific statement of consent.

10. DUTY OF CONFIDENTIALITY

Our staff and governors abide by a common law duty of confidentiality. This means that personal information that has been given to a member of staff or a governor by an individual should not be used or disclosed further, except as originally understood by that individual, or with their permission. Our staff and governors are subject to a Code a Conduct relating to confidentiality, and this policy should be read in conjunction with the Trust's Confidentiality Policy.

11. INFORMATION ABOUT CRIMINAL OFFENCES

The processing of information about criminal allegations, convictions or offences by each Academy is in accordance with our legal obligations and because we have legal authority in certain areas.

12. SURVEILLANCE

Each Academy may operate CCTV for protection of premises and to support any student behavioural issues. Campsmount Academy has a video surveillance system (VSS): a TCP/IP system.
We operate under a Code of Practice prescribed by the Information Commissioner's Office (ICO), and this policy should be read in conjunction with the Trust's CCTV Policy.

13. CHILDREN

Each Academy pays particular protection to the collecting and processing of children's personal data because they may be less aware of the risks involved. Where we offer an online service, which is not a preventive or counselling service, directly to a child, only children aged 13 or over are able provide their own consent. For children under this age we obtain consent from whoever holds parental responsibility for the child. The Trust has a competency test in place for children over the age of 13, in order that they understand what data may be released if a subject access request is made by a parent/carer. (Appendix 1)

14. SAFEGUARDING

The Trust understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.
The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared

- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

15. CLOUD COMPUTING

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

16. DBS DATA

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

17. AUTOMATED PROCESSING

Under the Data Access & Use Act 2025, the school recognises that personal data may be processed using automated systems, including artificial intelligence (AI), for certain administrative or educational purposes.

The school will only use automated processing or decision-making where it is lawful, fair, and necessary for a defined purpose, such as timetabling, assessment analysis, or safeguarding alerts. Any automated decision that could have a significant effect on an individual (for example, affecting a pupil's access to education or support) will include meaningful human oversight and review before a final decision is made.

Automated systems will not be used to make decisions based solely on special category data unless explicit consent has been obtained or another lawful condition applies.

The school's Data Protection Officer (DPO) will maintain oversight of all automated systems to ensure transparency, accuracy, and compliance with the principles of the UK GDPR and the Data Access & Use Act 2025.

18. HOW WE HANDLE PERSONAL INFORMATION - PRIVACY NOTICES

Each Academy provides privacy notices, which are statements to individuals about the collection and use of their personal data. The information includes our purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This information is on each Academy's website, and individuals are referred to it at the time we collect their personal data from them.

Where we obtain personal data from other sources, we provide individuals with privacy information within a reasonable period of obtaining the data but no later than one month after that time.

19. INDIVIDUAL RIGHTS

Individuals whose data is processed by an Academy have a number of rights in law:

1. The Academy will respond to a request by an individual for access to the information we hold about them. We will aim to respond within one month, however, we may take longer than one month and up to three months if the request is complicated, and we will inform you of this. There is no charge for this service. We will provide the information in secure electronic format unless you prefer otherwise. We will explain why we process your data, the lawful basis for doing so, who sees it and how long we keep it for.
2. The Academy can request that the data subject clearly specifies what data they are requesting. This may include time frames or types of data e.g. emails
3. The Academy is within their rights to pause the 28 day response if it needs further clarification of what data is requested
4. The Academy will respond within one month to a request from an individual to have personal data erased. Where the Academy can lawfully refuse to erase the data, we will explain why.
5. The Academy will respond within one month to a request from an individual to move, copy or transfer personal data easily from the Academy's computer network to another in a safe and secure way. We will do this in a structured, commonly used and machine readable form and free of charge.
6. The Academy will consider a request from an individual objecting to the processing of their personal data in relation to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

We shall ensure that individuals know about their right to object when we first tell them about the processing and in our privacy notice.

20. INFORMATION SHARING

The Academy believes that the duty to share information can be as important as the duty to protect information. We have a signed Information Sharing Protocol setting out the principles of information sharing with partners, such as the police, probation, prisons, Department of Work and Pensions, and the Department of Communities and the Local Authority.

This protocol is supplemented by Information Sharing Agreements at the point at which data is shared. These set out what data is being shared, how it is transferred and the retention period.

The Trust will ensure that any third parties which process data on its behalf ('data processors') meet the requirements set out in article 28 of the GDPR. Supplier contracts where the trust passes data to them, and they receive and store it, such as insurers, payroll and curriculum enrichment providers, are data processors.

The Trust Data Protection Lead is responsible for ensuring that these are compliant with the GDPR
At each Academy the School Business Manager will ensure that all such existing or new third party suppliers are compliant with data clauses as detailed in paragraph 3 of article 28.

21. TRANSFERS TO OTHER COUNTRIES

Most of our processing occurs in the UK or European Union. This means that there are common standards for the processing of personal data. However, when personal data is transferred to third countries, the Academy assures itself that there is a level of adequacy in the data protection arrangements of that country.

22. PRIVACY BY DESIGN

The Trust is committed to a privacy by design or privacy by default approach to building new systems and updating procedures for processing personal data. We use the best technology and human processes we can in order to limit the risks to privacy.

23. DATA PROTECTION IMPACT ASSESSMENTS

Each Academy carries out Data Protection Impact Assessments (DPIAs) when they introduce new technology or changes to the processing of personal data. The assessment identifies the risk to privacy from the customer's perspective and what steps can be taken to reduce this wherever possible whilst providing a service to the customer. We will consult all affected individuals. We will publish DPIAs on our website. We will treat them as living documents to be revised and updated whenever necessary.

24. CONTRACTORS

Where the Academy has a contractual relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information.

25. INFORMATION SECURITY

Each Academy has an Information Security policy. The purpose of this policy is to take appropriate technical and organisational measures to protect personal data.

26. BREACHES

Each Academy endeavours to prevent information breaches, but when these occur, there is an incident reporting procedure. Breaches are reported to the Data Protection Lead, Headteacher/Principal and Board of

Governors. Where a breach is a serious risk to the rights and freedoms of anyone, it will be reported to the Information Commissioner within 72 hours.

27. DATA PROTECTION OFFICER (DPO)

Schools are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staf f understand and are acting in accordance with relevant data protection laws.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

Leger Education Trust has appointed a Data Protection Officer as required by law. Their role will be to ensure the compliance of each Academy with data protection law. The Data Protection Officer is Tim Pinto and can be contacted by email tpinto@esafetyoffice.co.uk

Additionally, the Trust has appointed a Data Protection Lead, Rebecca Grange, Executive Director of Operations who can be contacted by email info@legereducationtrust.com

28. HOW TO COMPLAIN

If you think we have breached data protection, you can complain. The complaint will be investigated by the Data Protection Lead. We will respond within one month. If you are still unhappy, the Data Protection Officer will consider your appeal. Their response will take up to one month. Finally, individuals can take their complaint to the Information Commissioner's Office for a decision.

29. SERVICE AND BENEFIT

Data protection is a big challenge when digital technology can collect and transmit huge volumes of personal data. For our staff and governors, we are positive about the benefits, and serious about our responsibilities. We are transparent and accountable, and we believe that we can both serve, and protect, the information of our employees, governors, parents and students.

30. REFERENCES

Regulation (EU) 2016/679 (General Data Protection Regulation)
Data Protection Act 2018
Directive (EU) 2016/680 Law Enforcement Directive
Information Commissioner's Office: www.ico.org.uk

APPENDIX 1

Data Protection Competency Test

Test to be conducted with young person aged between 13-16 in relation to the request to release data by a parent/carer making a subject access request.

Date Of Meeting	
Meeting Conducted By	

Date Subject Name	
Date Of Birth	
Age	
SEND	

In line with Data Protection Law, young people over the age of 13 should be consulted about the release of data. This is in line with the Gillick Competency test:

Gillick Competency

The means by which to assess legal capacity in children/young people under the age of 16 years, established in the case Gillick v West Norfolk and Wisbech Area Health Authority (1985). Such children/young people are deemed to be capable of giving their own consent to advice or treatment without parental knowledge or agreement, providing they have sufficient understanding to appreciate the nature, purpose, likely effects and risks, chances of success and the availability of other options.

Age and Capacity

The law distinguishes between young people aged 16 to 17 years and children under 16 in respect of the capacity to consent.

Young people aged 16 to 17 - young people aged 16 and over in England are presumed in law to have the same capacity as an adult to consent or refuse advice, interventions, treatment and to the release of information. They do not therefore require parental consent unless there is a reason to believe that they lack capacity.

Children aged 13 to 15 - Capacity to consent needs to be assessed in each case on a continual basis. Children aged 13 to 15 can only consent if they are assessed as having the maturity and intelligence to fully understand the nature of the advice, intervention and treatment, the options, the risk involved and the benefits. A child who has such an understanding is considered to be Gillick competent.

Children 12 and under - there is no lower age limit for Gillick competence or Fraser guidelines to be applied. It would rarely be appropriate or safe for a child to consent to advice/intervention/treatment without parental consent. When it comes to sexual health those under 13 are not legally able to consent to any sexual activity. Therefore any information that a person under 13 is sexually active would need to be acted on.

Children under the age of 16 who are not Gillick competent cannot give or withhold consent. A person with parental responsibility will need to consent on their behalf unless it is an emergency or a safeguarding concern.

Definition of Subject Access Request

Individuals have the right to access and receive a copy of their personal data, and other supplementary information.

A parent/carer has asked to access data about them and as they are aged 13 or over, they need to be consulted about releasing the data.

Please detail the data the parent/guardian has requested

Competency Assessment Checklist

Complete with all young people, under 16years and 16 and above if there is a reason to believe that they lack capacity, this is to demonstrate competence to consent.

	YES	**NO**
The ability to understand that there is a choice and that choices have consequences		
The ability to weigh the information and arrive at a decision		
To communicate that decision		
A willingness to make a choice (including the choice that someone else should make the decision)		

An understanding of the nature and purpose of the proposed intervention		
An understanding of the proposed intervention's risks and side effects		
An understanding of the alternatives to the proposed intervention, and the risks attached to them		
Freedom from undue pressure		
Ability to retain the information		

Any additional notes related to the meeting

Subject Name	**Date**	**Signature**
Member Of Staff Name	**Date**	**Signature**