Data Protection Policy

Version	1.2
Name of Policy Writer	J. Webb
Written	April 2018
Updated/Reviewed	1. **J. Webb Sept 2020** – Policy amended to include appendices and DfE model updates 2. **D. Armitage Jan 2022** – Policy reviewed in line with data protection audits and to reflect changes to legislation following Britain's exit from the EU. 3. **J.Webb Sept 2023** – Policy updated to provide clarity on Safeguarding and Data Impact Assessments.
Next Review	September 2024

Contents

Appendices

1.0 Statement of Intent

Together Learning Trust and the schools within it aim 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 UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2.0 Scope and Legal Framework

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with our funding agreement and articles of association.

3.0 Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 The Data Controller

The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Together Learning Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.0 Roles and Responsibilities

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

5.1 Trust Board

The Together Learning Trust board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will be 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 staff understand and are acting in accordance with relevant data protection laws.

They will provide an annual report of their activities directly to the Together Learning Trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust schools process, and for the ICO.

Our DPO is Janine Webb, Director of Business, Operations and Compliance for Together Learning Trust. She is contactable via the Trust Central Team, c/o Brooksbank School, Victoria Road, Elland, HX5 0QG

5.3 Headteacher

The headteacher of each school within the Trust acts as the representative of the data controller on a day-to-day basis, ensuring effective implementation of this policy.

5.4 School Data Protection Lead

The Data Protection Leads in each school fosters a culture for protecting information and data and provides a focal point for managing information risk and information assurance. The Data Protection Lead will also be the conduit between the school and the DPO, providing information and updates as required and helping to facilitate trust QA processes regarding data protection.

5.5 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the schools of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

If they need help with any contracts or sharing personal data with third parties.

6.0 Data Protection Principals

The UK GDPR is based on data protection principles that our schools must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7.0 Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that schools can **fulfil a contract** with the individual, or the individual has asked a school to take specific steps before entering into a contract
- The data needs to be processed so that a school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that a school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of a school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, Minimisation and Accuracy

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.

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.

Staff must only process personal data where it is necessary in order to do their jobs.

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 Trust's record retention schedule/Records Management Policy.

8.0 Sharing Personal Data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- 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:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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.

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.

9.0 Subject Access Requests and other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This 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, or if this isn't possible, the criteria used to determine this period
- 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 made verbally or in writing, either by letter, email or fax to the DPO.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

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

9.2 Children and Subject Access Requests

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.

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 a school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- 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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- 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
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10.0 Parental Requests to see the Educational Record

Parents, or those with parental responsibility, can access their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11.0 Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the DPO to seek their opinion as to whether the processing operation complies with the UK GDPR.

12.0 Photographs and Videos

As part of our activities, we may take photographs and record images of individuals within our schools.

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.

Uses may include:

- Within schools on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of schools by external agencies such as the school photographer, newspapers, campaigns
- Online on school websites or social media pages

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.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.0 CCTV

The Trust uses CCTV in various locations around the school sites to ensure they remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to the individual schools of the Trust.

14.0 Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- 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

15.0 Data Security and Storage of Records

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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school offices
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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.

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).

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 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.

16.0 Data Retention and Disposal of Records

Personal data will be kept in line with the Records Management Policy and Retention Schedule. 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.

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

17.0 Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on a school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18.0 Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19.0 Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary, following any changes to legislation. Otherwise, or from then on, this policy will be reviewed annually and shared with the Trust board and Trust Schools.

20.0 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 Trust 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 Trust 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.

21.0 Links with other Policies

The Data Protection Policy is to be used in conjunction with;

- TLT Privacy Statements
- Freedom of Information Policy
- ICT Policy / Cyber Security Policy / ICT Acceptable User Agreement
- Records Management Policy and Records Retention Schedule
- Safeguarding and Child Protection Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider 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 DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, 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)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach 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 must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within the school office.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach 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
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO 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 DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO 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 DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - 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)

  Records of all breaches will be stored within the school

  The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Data Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 - 7 with as much information as possible and pass the form on to the Headteacher immediately. The breach will be recorded on the School's Breach Register and the DPO informed so that an investigation can be carried out if required.		
	Report by:	
	Date	
1	Nature of breach e.g. theft/disclosed in error/technical problem	
2	How did the breach occur?	
3	When was the breach reported and how did you become aware?	
4	Full description of all personal data involved	
5	Number of individuals affected? Have individuals affected been informed	
6	What immediate action was taken:	
7	Has the data been retrieved or deleted? If yes – date and time:	
8	Any Procedure changes needed to reduce risks of future data loss	
9	Final conclusion and outcome	

Appendix 3: Subject Access Request Form

1. *YOUR DETAILS (BLOCK CAPITALS PLEASE)

Surname:	First names:
Title:	Any other names used (e.g. maiden name):
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Daytime telephone number:	
Email address:	

*****You will be asked to provide proof of your identity and address. Please see the Guidance Notes attached.

2. WHOSE INFORMATION ARE YOU REQUESTING? (Please tick relevant box)

- **My own** ☐
- **Someone else's** ☐
- **Both my own and someone else's** ☐

3. *IF YOU ARE REQUESTING SOMEONE ELSE'S INFORMATION, TO WHOM DOES IT RELATE? (Please provide their details)

Surname:	First names:
Title:	Any other names used (e.g. maiden name):
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Daytime telephone number:	
Email address:	

Your relationship to this person (please tick the relevant box)

- Mother ☐
- Father ☐
- Carer ☐
- Other (please explain below) ☐

You will be asked to provide proof of entitlement to request information on someone else's behalf.

Please see the Guidance Notes attached.

4. DETAILS OF THE INFORMATION YOU ARE REQUESTING:

Please describe the type of information you want to see:

Which people do you think hold the information you are requesting?:

5. PROOF OF IDENTIFICATION AND ENTITLEMENT

Documents provided as proof of identity (please see the Guidance Notes):

- Passport or photo ID driving licence ☐
- Birth certificate ☐
- Bank statement ☐
- Recent utility bill (original, less than 3 months old) ☐
- Change of name documents (original) ☐

Signature of applicant:	Date:

Subject Access Request Guidance Notes

1. **Personal Details:** Please complete your personal details as requested. Please tell us if you have been known by any other name and if you have lived at your previous address for less than two years please provide your previous address. If you are requesting historical information, then provide as many details as possible, for example previous addresses with dates. Use a separate sheet of paper if required.

2. **Details of the information you require:** You should give as much detail as possible about the information you want us to provide and the people you think might hold the information to assist us in our data search.

3. **Proof of identification:** Proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, e.g. a recent utility bill (less than three months old) or a bank statement showing your name *and* address and an original piece of photo documentation such as a passport or photo ID driving licence. If you have changed your name please provide proof of this. All documents must be originals, photocopies will not be accepted.

4. **Keep your documents secure:** Documents may be brought into school or sent to us in the post. Always send these important original documents by Recorded, Special or Registered post. The school cannot be held liable for any documents lost in the post.

5. **Proof of entitlement**: Under the Data Protection Act, only the data subject has the right to ask to see their own records. All individuals aged 16 or over should make their own subject access requests if they have the mental capacity to make their own decisions (in this context mental capacity is defined as in the Mental Capacity Act 2005) unless they appoint someone else to make the request on their behalf.

6. **Making a request on behalf of someone else:** People making subject access requests on behalf of someone else need to demonstrate that they have the right to do so and we have listed the categories and proof required below. *****Please note that if you make a subject access request on behalf of a child or young person aged 12 to 15 years old, we may independently seek their consent to release the documents to you, even if you have parental responsibility for them. This means we may not disclose the information to you if they refuse their consent.

7. **A birth parent making a subject access request on behalf of their child aged below 16 years:**

   - **Birth mother:** Child's birth certificate.

   - **Birth father (married to the birth mother of the child):** Child's birth certificate and birth parent's marriage certificate.

   - **Birth father (unmarried to the birth mother of the child) for children born before 1 December 2003:** Child's birth certificate showing registration or re-registration of the birth after 1 December 2003 naming the birth father as the child's father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

   - **Birth father (unmarried to the birth mother of the child) for children born after 1 December 2003:** Child's birth certificate naming the birth father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

8. **An adoptive parent making a subject access request on behalf of their child aged below 16 years.**

   - The Adoption Order

9. **A person who is not the child's parent making a subject access request on behalf of their child aged below 16 years:**

    - Residence Order granted by the Court **or**
    - Special Guardianship Order granted by the Court **or**
    - Proof of permission to make the subject access request, a signed letter or consent form from a person with parental responsibility and/or the child if the child is 12 years or older

10. **A person making a subject access request on behalf of a person aged 16 years or over**

    - We require proof of permission to make the request on their behalf, such as a signed letter or consent form from the person. We may contact the person for confirmation that we can release the information to you.

11. **A person making a subject access request on behalf of a person lacking mental capacity aged 16 years or over:**

    - For a young person aged 16 – 17 years old we require proof of parental responsibility, as given in sections 5 and 6, or if you are a carer as in section 7 we require a Residence Order granted by the Court or a Special Guardianship Order granted by the Court.

For persons aged 18 or over we require proof of a valid Lasting Power of Attorney **or** an Enduring Power of Attorney **or** proof of a Court appointed Deputyship.