The Family of Learning Trust

Data Protection Policy

This policy is non contractual and may be updated or changed by the Trust subject to consultation (if required)

Version	**01/26**
Name of Policy Writer	**The DP Advice Service Ltd**
Last Reviewed	**December 2025**
Next Review Due	**December 2026***

DATA PROTECTION SPECIALISTS

Contents Page

1. Introduction 3
2. Purpose and Scope of this policy 5
3. Relationship with other policies 5
4. Responsibilities and requirements 5
5. Data Principles, Collection and Processing 6
6. Privacy Notices 8
7. Data Protection Officer 8
8. Individual's Rights 9
9. Subject Access Request 10
10. Data Protection Impact Assessments 11
11. Data Breaches 11
12. Consent 12
13. CCTV 12
14. AI 12
15. Data Security and Data Sharing 13
16. Remote working 14
17. Breach of Policy 14
18. Information Commissioners Office and Notification 14
19. Complaints Process for Data Rights 15
20. Review 15

Appendix One: The process if an individual exercises one of their rights 16
Appendix Two – Subject Access Requests 17
Appendix Three – Subject Access Request Form 19
Appendix Four – Subject Access Request Information 23
Appendix Five – Data Breach Procedure 25
Appendix Six – Data Rights Complaints Process 26

1. Introduction

1.1 It is necessary for us to collect personal data relating to pupils, parents, staff, governors, service providers and external agencies who work with us to carry out our function as a school.

1.2 In some instances, we may also be required by law to collect certain specified personal data to comply with the requirements of relevant central government departments.

1.3 The school is registered as a data controller meaning that it is legally responsible for handling (both storing and processing) such information in accordance with legislation. We can also

1.4 All personal information held by the school will be stored and handled in accordance with the Data Protection Act 2018 ('DPA'), the General Data Protection Regulations 2018 ('GDPR') and the Data (Use and Access) Act 2025.

1.5 The school ensures that when sharing any data with third parties (e.g. payroll providers, external HR providers, educational software solutions or other service providers) that those third parties are compliant with the relevant data protection laws and the information is shared securely.

This policy sets out the following information:

- Definitions of key terms used in the policy,
- The purpose and scope of the policy,
- The responsibilities and requirements on the school,
- The data principles and information relating to data collection and processing,
- Information relating to privacy notices,
- Information regarding the role of the Data Protection Officer,
- Individual's rights,
- Subject access request,
- Data Protection Impact Assessments,
- Data breaches,
- Consent,
- CCTV,
- AI
- Data Security and Data Sharing,
- Remote working,
- Details relating to the implications of breaching the policy,
- ICO and notification obligations.
- Complaints process for data rights.

Definitions

Data Controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of the personal information in either digital or paper format (or both). A data controller determines the purposes and means of processing personal data .
Data Processor	A data processor is responsible for processing the personal data on behalf of the data controller. Data processors must maintain records of the personal data they process and their processing activities.
Data Protection Legislation	The Data Protection Act 2018 and the General Data Protection Regulations 2018 and any other legislation from time to time in force.
Data Subject	The person who the personal data belongs to.
Information Commissioners' Office (ICO)	The office responsible for monitoring compliance with data protection laws and investigating and penalising data breaches.
Personal data	Personal data is any information relating to an identified or identifiable natural person (data subject), which would allow you to identify (or makes it possible to identify) that person.
Processing	Processing refers to the recording, handling, using, storing and sharing of personal data.
Subject Access Request	A data subject's right to request access to the information that a company or organisation holds about them, including why that information is held, what they do with that information, where it is stored, how long it is held for and who it is shared with .
Data Protection Impact Assessment (DPIA)	A process to help identify and minimise the data protection risks of a project which involves data processing; particularly useful when introducing a new data processing process, system or technology.

2. Purpose and Scope of this policy

2.1 This policy ensures that the school and its employees are aware of the relevant data protection legislation in force and are handling data in compliance with it.

2.2 In the course of their work, most employees (depending on their role) will be required to take part in the acquisition, recording, handling, storage and/or processing of personal data and this must always be done in accordance with this policy and the relevant legislation as outlined above.

2.3 This policy will help those employees understand the meaning and significance of such legislation and ensure they carry out their role in compliance with such legislation.

2.4 The school will ensure that (in addition to those employees directly involved in the handling of data) all members of staff, governors, volunteers, trainees, external contractors and/or consultants and any partners of the school who may have access to any personal data will receive appropriate information and/or training to make them fully aware of their individual and corporate responsibilities in this regard.

2.5 Such information or training will include making all employees (and others listed in the preceding clause) aware that breaches of data protection legislation have the potential to expose both the individual and the school to possible legal action (both criminal and civil).

2.6 This policy should be approved by the Trustees and read by all employees, volunteers, contractors, and other third parties when handling personal data controlled by the school. The policy should be made available on the school website.

3. Relationship with other policies

This policy should be read in conjunction with the following policies:

- Privacy Notices
- Freedom of Information Policy
- Record Management and Retention Schedule
- IT/Staff Acceptable Use Policy

4. Responsibilities and requirements

4.1 As a data controller, the school is responsible for ensuring that it only collects the required data necessary to carry out its role as an educational provider. The school recognises that obtaining additional data to that which is necessary is contrary to the Data Protection Laws.

4.2 The school is responsible for obtaining, storing and handling that data in a secure manner and will keep records of what data is held and the purposes for which it is held.

4.3 The school is responsible for ensuring that it only shares data with third parties where this is necessary for providing the full educational experience for the children, including meeting safeguarding obligations, reporting to local or central Government, ensuring staff employment rights are met and providing access to the best educational resources. The school is required to ensure that it only shares that data which is required by the third party for performing its function and it shares this data in a secure way.

4.4 The school is responsible for ensuring that any third party accessing or processing data controlled by the school will do so in a safe and secure manner and in compliance with the data protection laws in force.

4.5 The school is required to notify data subjects as to the personal data they hold in relation to that data subject as well as the legal basis for holding that data, how the data is used, who the data may be shared with and how it is stored. This is done in the privacy notices (please see the section of this policy entitled 'Privacy Notices' for further information).

4.6 The school is required to appoint a Data Protection Officer ('DPO'). More information about the role of the Data Protection Officer is set out under the section entitled 'Data Protection Officer' below.

4.7 The school is required to register itself as a data controller with the Information Commissioners Office and is responsible for any associated fee.

4.8 The school is required to obtain full records of all personal data held and maintain these records in accordance with the Records Management and Retention policy.

4.9 The school has an obligation to deal with any subject access requests in a timely manner (further information regarding this is set out under the Subject Access Request section below).

4.10 The governing body/board has overall responsibility for ensuring that the school complies with its obligations under the relevant data protection laws and this policy.

5. Data Principles, Collection and Processing

5.1 Article 5 of GDPR sets out the seven data protection principles which the school must comply with. These principles state that personal data must be:

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

The final principle is:

- **Accountability – it is everyone's responsibility to ensure the above principles are adhered to.**

5.2 When collecting personal data from parents/children/staff/third parties, the school must only collect the personal data necessary for the purpose that the data is required.

5.3 The school must have a valid lawful basis for collecting and processing personal data. There are now seven lawful bases available, and most require the processing to be necessary. The school must determine the appropriate lawful basis for collecting and processing the personal data prior to collection.

5.4 The lawful bases are:

Consent	The individual has given clear consent for the school to process their personal data for a specific purpose.
Contractual	The processing is necessary a contract you have with the individual or because they have asked you to take specific steps before entering a contract.
Legal Obligation	The processing is necessary for you to comply with the law (not including contractual obligations).
Vital Interests	The processing is necessary to protect someone's life.
Public Task	The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate Interest	The processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks – this would be covered by another basis).
Recognised Legitimate Interests	The Data (Use and Access) Act 2025 has introduced a new lawful basis called recognised legitimate interests. This differs from the legitimate interest basis under the Data Protection Act as it removes the need to balance the impact on the people whose personal information you use, against the benefits arising from that use. It is particularly used for data sharing for safeguarding or criminal/legal investigation purposes.

5.5 The school must only then use the personal data for the purpose for which it has been collected. If they require the use of that personal data for another purpose, they must contact the data subject to notify them of this.

5.6 The personal data collected must be kept in compliance with the Records Management and Retention Policy.

5.7 If the school uses any third parties for processing personal data (e.g. progress tracking systems) then it is the school's responsibility to ensure that the third party complies with data protection laws when processing that data. This responsibility will be met by checking that the third party have the required compliance measures and safeguards in place to protection personal information. It may be necessary to complete a Data Protection Impact Assessment (DPIA).

6. Privacy Notices

6.1 Privacy notices should be prepared to inform the data subjects about the data processing the school carries out.

6.2 Privacy notices must include information such as the personal data required, why that personal data is required, what the personal data will be used for, how the personal data will be stored/shared/processed, who the DPO is and the rights that an individual has in relation to their personal data.

6.3 Privacy notices should be prepared for any personal data obtained by the school but will most commonly be split into privacy notices for parents/children, a privacy notice for staff/volunteers/contractors and a privacy notice for job applicants.

6.4 The school should ensure that the data subject has access to the privacy notice, e.g. by publishing the relevant privacy notices on to the website.

7. Data Protection Officer

7.1 The school is a public authority for the purposes of the DPA and therefore requires a DPO.

7.2 A DPO should be appointed by all schools in England, and the officer should be independent from the processing of personal data.

7.3 The DPO should have specialist knowledge of data protection laws and the requirements on the school for compliance. They should be able to advise and influence the senior leadership of the school.

7.4 The DPO will assist the school in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments ('DPIA')(see the section on this further on in this policy) and act as a point of contact for data subjects and the supervisory authority (ICO).

7.5 The DPO's details must be made available to the data subjects, this is done through the privacy notices.

7.6 The school can refer to Article 39 GDPR for a further definition of the tasks of the DPO.

8. Individual's Rights

8.1 The GDPR provides the following rights for individuals:

The right to be informed	About the collection and use of their personal data. The key is that the school needs to be transparent about the collection and use of personal data. This information is set out in the privacy notice.
The right of access	See the Subject Access Request section of this policy at Section 9 below.
The right to rectification	This provides the right to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request to rectify either verbally or in writing and the school will have one month to respond to that request.
The right to erasure	(also known as the right to be forgotten). This is not an absolute right and only applies in certain circumstances. An individual can make a request, and the school would have one month to respond to such a request. The school should refer to its Records Management and Retention Policy for further information about deleting personal data.
The right to restrict processing	Individuals have a right to request the restriction or suppression of their personal data in certain circumstances. Again, this is not an absolute right and only applies in certain circumstances. When processing is restricted, you are only permitted to store the personal data but not use it.
The right to data portability	This gives the individual the right to obtain and reuse their personal data for their own purposes across different services.
The right to object	Gives an individual the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In order circumstances the school will be able to continue processing personal information if there is a compelling reason to do so.
Rights in relation to automated decision making and profiling	(this refers to deciding solely by automated means without any human involvement). Profiling is automated processing of personal data to evaluate certain things about an individual.

8.2 All individuals have the rights set out above. If the school receives a request in relation to any of the above rights, then they should contact the DPO for further advice. A procedure for dealing with such requests is set out at Appendix 1 to this policy.

9. Subject Access Request

9.1 A Subject Access Request is the term used for an individual's right to request to view their personal information that is held by the school. It is also known as the right of access referred to at 8.1 of this policy.

9.2 A data subject has the right to find out what data is held on them and how it is used. An individual should make a Subject Access Request before exercising the other information rights set out in section 8 above.

9.3 Subject Access Requests can be made verbally or in writing but, to assist individuals in making such requests, the school has prepared a subject access request form which can be obtained from the school office and is referred to in the procedure in Appendix 2 below or can be found at Appendix 3.

9.4 The school must respond to any Subject Access Request within one month of receipt of such request. The school should contact the DPO if they receive a Subject Access Request. It is possible to extend this period for a further two months if the volume of data in the request is significant.

9.5 The school is only obliged to provide information relating to the data subject and cannot provide any personal information which may identify another individual unless the school has that individual's consent. The school is also not permitted to provide any personal information that may be capable of identifying an individual other than the requesting data subject.

9.6 The school should provide a copy of the privacy notice or refer the data subject to the privacy notice on the website, as well as providing the information, as part of the subject access request.

9.7 The school should keep a record of all Subject Access Requests; the record should include details about the date of the request and the date of the response.

9.8 The school can refuse to provide information as part of a Subject Access Request in certain circumstances, for example, the information has been provided following a previous request and there have been no changes to the information held or the way it is processed since that initial request. Where the school refuses to provide information requested it must document this and the reasons for the refusal. In this instance the request would be manifestly unfounded.

9.9 The school may also refuse to respond to a request if it is manifestly excessive.

9.10 Personal data about a child belongs to that child and not the child's parents/carers. Parents can make a Subject Access Request on behalf of their child where the child is unable to understand their rights and the implications of a Subject Access Request. Children under 13 years old are generally not considered mature enough to understand these rights although each case ought to be considered on its facts.

9.11 The procedure for what to do if you receive a Subject Access Request is set out in Appendix 2 to this policy.

10. Data Protection Impact Assessments

10.1 A Data Protection Impact Assessment (DPIA) should be carried out when the processing of data is likely to result in a high risk to the individuals. It is good practice to carry out a DPIA when carrying out activities that require data processing.

10.2 The DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures in place; identify and assess risks to the individual and identify any additional measures to mitigate those risks.

10.3 Once the DPIA has been carried out the school should sign off the project/activity requiring the data processing and record the outcomes of the DPIA.

10.4 In carrying out your DPIA, you should seek advice from DPO, where necessary.

10.5 It is important to keep a record of your DPIA for each activity.

10.6 If a risk to personal information is identified in the DPIA and the risk cannot be mitigated against then the school must contact the ICO before proceeding with the activity.

11. Data Breaches

11.1 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. It includes breaches which resulted from both accidental and deliberate causes.

11.12 If anyone within the school suspects that there has been a data breach, they must report this to the DPO and Senior Leadership Team as soon as possible.

11.3 Any breach which is likely to result in a high risk of adversely affecting an individuals' rights and freedoms will need to be reported to the ICO, within 72 hours of becoming aware of that breach.

11.4 In assessing risk to the rights and freedoms the school should have regard for Recital 85 GDPR.

11.5 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the school must inform those concerned directly and without undue delay.

11.6 The school must keep a record of all breaches, whether reported or not. If a breach has not been reported, a record must be kept of the reasons for not reporting.

11.7 The procedure for dealing with a data protection breach is set out in Appendix 5.

12. Consent

12.1 The school must obtain consent from parents/pupils for obtaining and processing certain personal data such as the use of photographs (particularly for marketing purposes such as brochures and websites).

12.2 The consent must be freely given, specific, informed and unambiguous and confirmed by a statement or clear affirmative action.

12.3 A record must be kept of all consents provided.

12.4 A consent form must set out the ways an individual may be able to change or withdraw their consent.

12.5 The school must seek guidance from the DPO if it has any queries relating to obtaining consent.

13. CCTV

13.1 The school may use CCTV in and around school to ensure the safety of all children, visitors, staff and the protection of the property. The school must always comply with the ICO's code of practice for the use of CCTV.

13.2 We are not required to ask permission from individuals for using the CCTV, but we do make it clear that CCTV is in use. We do this by making the CCTV cameras clearly visible and by displaying signs explaining that CCTV is in use.

13.3 Whilst an individual may make a Subject Access Request to view CCTV footage, the school will need to consider the points made in clause 9.4 above in deciding whether it is appropriate to allow such a request. A copy of the footage will not be released to individuals.

14. AI

14.1 Artificial Intelligence (AI) is the use of computer systems to perform tasks that would ordinarily require human intelligence. Examples of some commonly used systems include ChatGPT or Google's Gemini.

14.2 AI has a knowledge bank which it takes from information available on the internet and the information that is entered into it by users. Every time someone enters something into AI, the entry and any information retrieved to provide the response, forms part of the systems knowledge bank.

14.3 AI can be used to assist with certain tasks such as creating a lesson plan, drafting a letter or policy, research or providing general information about an activity.

14.4 You should not enter any personal information into AI as the security and confidentiality of that data cannot be protected. For example, if you are using AI to create a seating plan for your classroom you could enter the number of students, the number of girls and boys, the fact that you would like x number of students per table in a ratio of x girls to x boys and even that you have two pupils who will need to be separated or sat together but you would need to call these pupils x and y rather than using their names.

14.5 You should be transparent about AI tools that are being used in school. Information can be set out in the privacy notices. It is important to make clear that personal data will not be entered into AI systems.

15. Data Security and Data Sharing

15.1 The school will ensure that all data is collected, stored, processed and shared in a secure manner; whether the data is held in electronic or paper format.

15.2 The school will ensure that any digital sharing of personal data is done in accordance with the IT/Staff Acceptable Usage policy.

15.3 Where data is shared with a third party who is responsible for processing that data for a particular purpose, the school must ensure that the third party is compliant with the GDPR and DPA.

15.4 The school must not share any personal information with anyone unless it has a legal requirement to do so or has obtained consent in advance. The most common data sharing that the school does is with the Local Authority and the Department for Education. Information on this sharing is set out in the privacy notices.

15.5 Other data sharing that the school may do without prior notice or obtaining consent would be where there is a safeguarding or medical need and we have not been able to contact the parent/carer/next of kin in advance or the law does not permit us to contact the parent/carer in advance. In these circumstances, we may need to share a child's or parent/carer's information with medical or other professional teams.

15.6 We may also share personal information with third parties who assist us in providing the best resources and support for a child's education. This may include software solutions and other digital services. The school must ensure that they are compliant with data protection legislation, and they are only sharing the personal data that they need to carry out the service.

15.7 In all other instances, the school would speak with the parent/carer first before sharing any personal information for that parent/carer or child. The school would ensure that it provides as much information as possible about what it proposes to share, why it is sharing that information and who it is sharing the information with.

15.8 If the school is sending information via email, it must ensure that it is secure and encrypted, where necessary, to safeguard the information contained/attached within.

15.9 If there is a need to transfer any personal information in hard copy, then care must be taken to first check whether the information could be delivered or collected in person and signed for on receipt. If this is not possible, the information should be sent by recorded delivery to ensure it can be tracked and signed on receipt. A receipt should also be sent so the organisation can complete it and return to say that they have received the information.

15.10 When any personal data sharing is carried out, staff must ensure that they comply with this Data Protection policy.

15.11 Any personal data that is no longer needed will be disposed of in line with the Records Management and Retention policy and will be disposed of securely.

16. Remote working

16.1 If a staff member is required to work remotely and that work involves the processing of personal data, then the staff member should ensure that such data is processed in a secure manner.

16.2 Remote working should be carried out on a password protected laptop/computer and where possible personal information should not be saved anywhere other than the secure school network.

16.3 When processing personal data remotely, staff should not allow other people to view the personal data.

16.4 When working remotely, if a staff member is required to share personal data, they should ensure that they adopt a secure method of data sharing and adhere to the basis for sharing as set out in the privacy notice.

16.5 Staff should have regard to the IT/ Staff Acceptable Use Policy and the Records Management and Retention Policy.

17. Breach of Policy

17.1 The Headteacher and the DPO are responsible for reviewing and monitoring compliance with this policy.

17.2 Any reports of staff, governors or third parties breaching this policy should be reported to the DPO and investigated fully. Any breaches will be taken seriously, and disciplinary action may be taken.

18. Information Commissioners Office and Notification

18.1 The school is registered as a data controller with the ICO and will renew this registration on an annual basis as required by the legislation.

19. Complaints Process for Data Rights

19.1 The Data (Use and Access) Act 2025 sets out that any complaints about data subject rights, including any data breaches, must be investigated by the data controller before escalation to the Information Commission.

19.2 The complaints process should sit outside the usual school Complaints Policy as it specifically relates to an individual's data rights and follows a different route of appeal.

19.3 The individual should use the complaints form set out in the appendix to this policy and submit this to school in writing. The school must investigate and respond to the complaint within 30 days of receipt of the complaint.

19.4 If the individual is not satisfied with the response provided by the school, then they have a right to appeal to the Information Commission.

20. Review

This policy should be reviewed on an annual basis.

The next review will be due in **December 2026**

Appendix One: The process if an individual exercises one of their rights

An individual may contact the school to request any of their rights set out in clause 8.1 of this policy. The request may be verbal or in writing and could be made to any member of staff.

If you believe that a request has been made by an individual for any of the rights set out in 8.1 of this policy, then please follow the procedure below when dealing with such a request.

Acknowledge receipt of the request as soon as possible (it may also be necessary at this stage to clarify your understanding of the request being made). The acknowledgement should be sent within 3 school days of receipt.

Speak to the Senior Leadership Team (SLT) and the DPO for advice about the request that you have received. It may not be possible (in law) to carry out the request so an assessment will need to be made of all the circumstances. You will need to pass the request to the SLT and DPO within 3 school days of receipt and confirm to the SLT and DPO that you have acknowledged receipt.

The DPO and SLT should consider the request as soon as reasonably practicable and should provide a response to the request within one month of initial receipt by the school/academy.

The school/academy should keep a record of all such requests made. The record should include the date of receipt, details of the request (which right was requested), the date of response and the outcome. If it is not possible to carry out the request, then the record should state the reasons why this was not possible.

The most common request likely to be received is the right to access (also known as a Subject Access Request). Further details on the process for dealing with a Subject Access Request are set out in Appendix Two of this policy.

Appendix Two – Subject Access Requests

An individual can make a Subject Access Request in any form whether verbal or in writing. The school/academy has a Subject Access Request form which they should encourage individuals to complete if they wish to make a Subject Access Request, but it is not necessary for the individual to use that form for their request.

When dealing with a Subject Access Request the school/academy should have regard to the procedure set out in Appendix One.

The school/academy should also note the following:

An individual is only entitled to their own personal data and, it may be necessary to establish the identity of the individual making the request before any information is provided.

If you need to confirm the identity of the individual making the request, you should ensure that you have seen a photographic form of identification such as passport or driving licence. You should ask for this straight away so that it does not delay your response.

You cannot provide personal data that may be capable of identifying another individual unless you have that individual's consent. It is therefore necessary to carefully consider all personal data on the subject requesting access prior to disclosure.

In addition to providing the individuals personal data you will also need to provide the following information:

- The purpose for which you process their personal information,
- The categories of personal information concerned,
- Information of any third parties that you share the personal information with,
- The retention period of storing the personal data or criteria for establishing the retention period,
- The existence of the other rights the individual has, set out in clause 7 of this policy,
- The right to complain to the ICO,
- Information about the source of the data, where it was not obtained directly from the individual,

- The existence of any automated decision-making (including profiling) of the personal data,
- The safeguards in place if and when the personal information is transferred to a third country or international organisation (this one is unlikely to apply to you).

When assessing what information to provide as part of a Subject Access Request you should first be guided by the request made and note that you will need to provide any records you have relating to the request including (but not limited to) records on SIMs, CPOMs, the child's file and emails.

In responding to the Subject Access Request, the school should use the subject access information form and ensure that any response is provided within one month. The time starts on the day the request was received but includes weekends and school holidays. You can extend this by a further two months if there is a large volume of data to process under the request.

You must review and redact/withhold any information that may be capable of identifying another individual (excluding staff members) and any information that could result in a safeguarding concern for any individual.

If you receive a request for 'all records held' and a reasonable search is carried out and a large volume of data is returned, it may be possible to ask the individual to narrow the scope of their request. You should seek assistance from your Data Protection Officer for this.

In some circumstances, it is possible to refuse to respond to a request if it is deemed to be manifestly excessive or unfounded. There is a high threshold to meet, and you should seek guidance from your DPO before relying on either of these.

Appendix Three – Subject Access Request Form

Subject Access Request Form

This form is for any person who wishes to apply for access to personal data held by [school name] only. Please read the Guidance Notes at the end of this document before completing this form.

A separate form should be completed for everyone.

Section 1: Your Details (Please complete the form in black ink in block capitals)

Surname:	First Name:
Title:	Previous names:
Date of Birth:	Contact Number:
Current Address:	Previous Address(es):
Email address:	

Section 2: Whose information are you requesting (please tick the relevant box)

My own personal information

Someone else's information

My information and someone else's information

Section 3: Third parties details (only complete this section if you are requesting access to someone else's information)

Surname:	First Name:

Title:	Previous names:
Date of Birth:	Contact Number:
Current Address:	Previous Address(es):
Email address:	

Please explain your relationship to this person (tick the relevant box below):

Mother

Father

Carer

Other

If you have selected other please explain:

Section 4: Details of the information you are requesting:

Please let us know what information you wish to receive – you may find it useful to refer to the checklist below: (please note that a request for a large volume of information may mean that we ask you to narrow the scope of your search to ensure that we can comply with your request)

Please let us know who you think may hold information that you wish to see:

Checklist:

Please use this checklist to help establish which information you wish to receive:

- Attendance data
- Attainment data
- Safeguarding records
- SEND records
- Behaviour records
- School reports
- Correspondence/communication

If you have requested to receive any correspondence/communication, please let us know as much information as possible e.g. which members of staff, what subject matters, whether you wish to receive letters or emails:

Section 5: Declaration:

I confirm that the information provided is true and accurate to the best of my knowledge and that I have the requisite authority to make this request.

Signature:	Date:

Guidance Notes

This form is not mandatory; you may request access to your information in other formats including verbally. This form is designed to speed up the process of the subject access request.

There is no fee payable to make a subject access request.

You will need to complete section 1, 2, 4 and 5. If you are a parent completing the form on your child's behalf, you must also complete section 3.

As part of the process, we may ask you to provide some form of identification; it may be that we ask you for two forms of ID with one form being photographic identification (either a passport or driving licence). Once we receive your request, we will notify you if we require you to provide your identification documents.

If you need help completing this form, please contact the Academy Trust or school office, and they can help you.

In addition to the right to have access to the information we hold about you, in certain circumstances you may also have other rights as set out in section 8 of the Data Protection Policy.

If you have questions about any of these rights please contact the Data Protection Officer, The DP Advice Service Ltd (info@thedpadviceservice.co.uk).

Please complete the personal details section(s) as requested. Please notify us if you or your child has been known by any other name. If you have lived at your address for less than two years, please also provide any previous addresses that we may have for you. If you are requesting historical information, please provide as much information as possible including previous names and addresses. Please use additional paper if necessary.

We have asked for details of the information you require – if you make a request for all the records held, we will provide you with all the personal data that we hold about you/your child that we are permitted under the data protection laws to provide. If the data volume is large, we may be required to ask you to narrow your request's scope. If there is something that you are specifically interested in obtaining, then please refer to this within the relevant section of the form.

The Data Protection Act 2018 only allows the data subject the right to request information held about them unless there are exceptional circumstances which mean that someone else can make that request on the data subject's behalf. The most relevant circumstances here will be where the child is under 13 years old and is unable to understand the data protection/subject access request process and its relevance.

If you make a request on behalf of your child, then we may request to see your entitlement to make such a request; this could involve asking to see proof of parental responsibility. If your child is over 13 years old, we will be required to obtain their consent before we can provide any information to you.

Appendix Four – Subject Access Request Information

Thank you for your subject access request which we received on [insert date]. Under the GDPR and Data Protection Act 2018, you are entitled to obtain a copy of the personal data we hold for you, the information about how and why we hold your data and, where relevant, who we share it with.

In this instance you requested personal information relating to [insert details here]. [We have obtained consent/we do not need to obtain consent from] [insert child's name].

You are entitled to the following:

- Confirmation that we are processing your personal data;
- A copy of the personal data requested; and
- Supplementary information which we have set out in our privacy notice pupils/parents.

We can confirm that we hold [insert name] personal data as a pupil of the school. Your request is for data specifically [set out details of what has been requested].

We hold the personal data as we have a legal obligation to provide the education/assessment for [insert child's name].

The type of personal data we hold about you/your child, why we hold this, the recipients or categories of recipients who we disclose this personal data to and information regarding the retention of this data, the rights you have to this data and your rights to lodge a complaint with the ICO are all set out in the [pupil/parent] privacy notice. A copy of which [is enclosed for your information][can be found on the school website – insert location].

The Data Protection Act 2018 states that we are not able to provide any personal data if it would mean disclosing information about another individual who can be identified from that information, except if:

The other individual has provided consent to the disclosure; or

It is reasonable to comply with the request without the individual's consent.

When deciding if it is reasonable to comply with the request without the consent we will take into account the following:

- The type of information that we would disclose;
- Our duty of confidentiality to that individual;
- Any steps we have taken to obtain the consent from that individual;
- Whether the individual is capable of providing consent; and
- Any express refusal of consent by the other individual.

We would also withhold information if you believed disclosure of the information could lead to a safeguarding concern.

In deciding on the above matters, we will balance your rights to receive information against the rights of, and our obligations to, the other individual.

Please find enclosed a copy of the personal data that we hold for your child. Please note that we have withheld/redacted some information that included details of other individuals that we were not able to disclose to you.

If you have any questions please contact the school's Data Protection Officer, The DP Advice Service (info@thedpadviceservice.com).

If you are unhappy with the way your request has been processed, you must submit a data rights complaint form to us, and we will have 30 days to investigate and provide a response. If you remain unhappy, have the right to raise a complaint with the Information Commissioner's Office by contacting 0303 123 1113.

Appendix Five – Data Breach Procedure

If you suspect a data breach has occurred, please follow the procedure set out below:

Report the suspected breach as soon as possible to a member of the Senior Leadership Team.

Make a written record of the suspected breach and the date it was reported to the SLT on the data breach log.

The SLT may wish to contact the DPO at this stage for advice.

The SLT/DPO should consider if any action is required to contain the breach if there is an ongoing threat to the security of personal data (e.g. if the computer systems have been hacked then consider changing passwords etc).

The SLT/DPO should investigate the suspected breach to establish how it happened and what the impact of the breach has been.

The SLT/DPO should consider whether the matter needs to be reported to the ICO. A data breach should be reported to the ICO unless you are satisfied that it is unlikely to result in a risk to the individual's rights and freedoms.

If a matter is to be reported to the ICO then the report needs to be made within 72 hours from being aware that a breach has occurred.

The SLT/DPO should consider whether they need to contact any individuals' to notify them of the breach and the action taken.

The SLT/DPO should record the outcome of the investigation and any action taken in the data breach log. They should include whether the matter was reported to the ICO and, if the matter was not reported to the ICO, it will need to include the reasons why.

Assess the procedure/issue which led to the breach and consider whether changes need to be made.

Inform your governing body regarding the data breach and resulting action taken.

Appendix Six – Data Rights Complaints Process

This process should be followed if an individual wishes to submit a complaint about one of their information rights (set out in Clause 8).

The individual should complete the complaints form set out in appendix 7 and return this to the school (insert email address).

School should appoint an appropriate person to investigate the complaint (this is likely to be the Data Protection Officer or member of the Senior Leadership team). The person may depend on the nature of the complaint and any personnel associated with the complaint.

The school should acknowledge receipt of the complaint and notify the individual who has been appointed to investigate the complaint.

A thorough investigation should be carried out, and a response must be provided in a timely manner.

The full investigation and response must be provided within 30 days of receiving the complaint.

If the individual has not completed the complaints form or provided sufficient information to carry out an investigation, the investigator will contact the individual to obtain further information. The 30-day period will commence from the date the further information is received from the individual.

Following the response from the school, the individual has a right to escalate the complaint to the Information Commission if they believe that their rights have been infringed and the outcome of the complaint does not address this.

Information Rights Complaint Form

Personal information:

Name:	
Child's name:	
Child's class:	
Email address:	

Details regarding the complaint:

Which of the following information rights does your complaint relate to (tick all that apply):

The right to be informed	About the collection and use of their personal data. The key is that the school needs to be transparent about the collection and use of personal data. This information is set out in the privacy notice.	
The right of access	See the Subject Access Request section of this policy at Section 9.	
The right to rectification	This provides the right to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request to rectify either verbally or in writing and the school will have one month to respond to that request.	
The right to erasure	(also known as the right to be forgotten). This is not an absolute right and only applies in certain circumstances. An individual can make a request, and the school would have one month to respond to such a request. The school should refer to its Records Management and Retention Policy for further information about deleting personal data.	
The right to restrict processing	Individuals have a right to request the restriction or suppression of their personal data in certain circumstances. Again, this is not an absolute right and only applies in certain circumstances. When processing is restricted, you are only permitted to store the personal data but not use it.	

The right to data portability	This gives the individual the right to obtain and reuse their personal data for their own purposes across different services.	
The right to object	Gives an individual the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In order circumstances the school will be able to continue processing personal information if there is a compelling reason to do so.	
Rights in relation to automated decision making and profiling	(this refers to deciding solely by automated means without any human involvement). Profiling is automated processing of personal data to evaluate certain things about an individual.	
Data breach	A data breach refers to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.	

Please provide as much information regarding your complaint as possible:

Please continue using additional sheets if necessary.

Please describe the impact this has had on you/your child:

Please let us know whether you would prefer to receive a response to your complaint via email or post:

Email

Post

Signed.....

Name.....

Date.....