Leeds Diocesan Learning Trust (LDLT)

Company Number 13687278

GDPR and Data Protection Policy

Policy Reviewed by Board of Directors: 06.03.2024
Date of Next Review: February 2027
Responsible Officer: CFO/CEO

Contents

Vision Statement		2
Related Policies		2
1.	Importance of data protection	2
2.	This policy statement	2
3.	Legal framework	3
4.	Applicable data	3
5.	Principles	3
6.	Accountability	4
7.	Data protection officer (DPO)	4
8.	Lawful processing	5
9.	Consent	6
10.	The right to be informed	6
11.	The right of access	7
12.	The right to rectification	7
13.	The right to erasure	8
14.	The right to restrict processing	8
15.	The right to data portability	9
16.	The right to object	10
17.	Automated decision making and profiling	10
18.	Privacy by design and privacy impact statements	11
19.	Data breaches	11
20.	Data security	12
21.	Publication of information	13
22.	CCTV and photography	13
23.	Data retention	14
24.	DBS data	14
25.	Appendix 1: Retention periods	15

Vision Statement

Serving and celebrating our unique schools and communities, we will love, live and learn together. Valuing our pupils, staff, governors and team as people of God, we will deliver transformational learning and the flourishing of all.

Related Policies

- Biometric Data Policy
- CCTV and Monitoring Policy
- Freedom of Information Policy
- Scheme of Delegation
- Privacy Notices
- Whistleblowing Policy

1. Importance of data protection

In order to operate as an organisation, we hold Personal Data about employees, suppliers, examination invigilators, volunteers, pupils and their family members, and carers and other individuals. The use of Personal Data is governed by the General Data Protection Regulation (the "GDPR"). We take data protection very seriously and understand the impact that data breaches and misuse of data may have on data subjects as well as on our activities. Compliance with this policy is necessary for us to maintain the confidence and trust of those whose Personal Data we handle.

Non-compliance with this policy by employees could in certain circumstances constitute a serious disciplinary matter. Training (including refresher training) is provided at induction and on a periodic basis. Staff and Volunteers are expected to maintain their knowledge and appreciation of data protection law and this will be supported by the organisation through, in particular, regular access to training. Please contact the Data Protection Officer if you feel that you require access to that course at any point. From time to time the Trust will require the successful completion of data protection training courses.

The operation of this Policy will be monitored by the Data Protection Officer who shall ensure that it is kept up to date. If you have any questions concerning this Framework or believe that it can be improved in any respect, please discuss with the Data Protection Officer.

2. This policy statement

The aim of this Policy is to give you a basic understanding of the data protection laws, our responsibility in respect of data protection practice, your rights and obligations and to explain why privacy is so important to us. It applies to all actions we take which involve the processing of and working with Personal Data.

The Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The Academy may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

3. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

4. Applicable data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

5. Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

6. Accountability

The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

Schools will provide comprehensive, clear and transparent privacy notices. Copies of the Trust privacy notices can be obtained on the website.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The Trust and schools will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

7. Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the Academy and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Academy's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee of the Trust has been appointed to the role of DPO. The current DPO is the Chief Financial Officer to the Trust. Each school will have an individual who is responsible for data protection within the school (Data Co-ordinator).

The individual appointed as DPO will have professional experience and knowledge of data protection law.

The DPO will report to the CEO. The Data Co-ordinator will report to the highest level of management at the school, which is the Headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their duties.

8. Lawful processing

The legal basis for processing data has been identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - Compliance with a legal obligation.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.
    - Protecting the vital interests of a data subject or another person.
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the Academy in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care

or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - 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 healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The Academy ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

10. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, schools will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Academy holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Schools will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Academy will ask the individual to specify the information the request is in relation to.

12. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. The right to restrict processing

Individuals have the right to block or suppress the Trust's processing of personal data.

In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust/ School has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust/ School is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust/ School no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the Trust/ School will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust/ School will inform individuals when a restriction on processing has been lifted.

15. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The Trust/ School will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Trust/ School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Trust/ School will consider whether providing the information would prejudice the rights of any other individual.

The Trust/ School will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Trust/ School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The right to object

The Trust/School will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust/School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust/School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Trust/School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust/School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust/School is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Trust/School will offer a method for individuals to object online.

17. Automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The Trust/School will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the Trust/School will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust/School has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

18. Privacy by design and privacy impact statements

The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust/School to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust'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.

A DPIA 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 Trust/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 Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

19. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Academy becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

20. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, schools enable electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff, directors and Governors will not use their personal laptops or computers for School/ Trust purposes.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust/School containing sensitive information are supervised at all times.

The physical security of the School's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Trust is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

21. Publication of information

Classes of information that will be made routinely available include:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified above are made available quickly and easily on request.

Neither the Trust nor the School will publish any personal information, including photos, on their websites without the permission of the affected individual.

When uploading information to the website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV and photography

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles and the CCTV and monitoring policy.

The School notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for a reasonable period of time for security purposes; the Headteacher or School Business Manager is responsible for keeping the records secure and allowing access.

The School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the School wishes to use images/video footage of pupils in a publication, such as the website, prospectus, or recordings of plays, written permission will be sought for the particular usage from the parent of the pupil.

Precautions are taken when publishing photographs of pupils, in print, video or on the Trust/School website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

23. Data retention

Data will not be kept for longer than is necessary.

See Appendix 1 for The Trust's suggested retention periods for pupil records.

Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24. 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.

25. Appendix 1: Retention periods for pupil records

Type of file	Retention period (operational)	Action taken after retention period
Admissions		
All records relating to the creation and implementation of the school's Admissions Policy	Life of the policy plus three years, then review	After the retention period, this information should be securely disposed of
Admissions (successful)	Date of admission plus one year	After the retention period, this information should be securely disposed of
Admissions appeals (unsuccessful)	Resolution of case plus one year	After the retention period, this information should be securely disposed of
Register of admissions	Three years after the date on which the entry was made	After the retention period, the record should be reviewed. Schools may wish to keep the register permanently as an archive record, as they are often contacted by past pupils to confirm the dates they attended the school, or transfer them to the appropriate LA archives service
Proofs of address supplied as part of the admissions process	Current academic year plus one year	After the retention period, this information should be securely disposed of

Supplementary information form including information such as religion. medical conditions, etc.	**If the admission was successful:** This information should be added to the pupil file **If the admission was unsuccessful:** Until the appeals process has been completed	After the retention period, this information should be securely disposed of
Pupils' educational records		
Pupils' educational record	Whilst the pupil remains at the school	After the retention period, the file should follow the pupil to the relevant destination, such as another primary school, a secondary school or a PRU The IRMS advises that schools may wish to retain the information about the pupil for a short period to allow for any queries or reports to be completed or where linked records in the school information management system have not yet reached the end of their retention period and deleting would cause problems If the pupil transfers to an independent school, leaves for elective home education, leaves the country or dies whilst at the school, the file should be returned to the LA and retained for the statutory period
Public examination results	Added to the pupil's record and transferred to their next school	All uncollected certificates should be returned to the examination board

Internal examination results	Added to the pupil's record and transferred to their next school	After the retention period, this information should be reviewed If the information is no longer needed, it should be securely disposed of
Behaviour records	Added to the pupil's record and transferred to their next school Copies are held whilst the pupil is at school plus one year	After the retention period, this information should be securely disposed of
Exclusion records	Added to the pupil's record and transferred to their next school Copies are held whilst the pupil is at school plus one year	After the retention period, this information should be securely disposed of
Child protection information held on a pupil's file	Stored in a sealed envelope for the same length of time as the pupil's record	After the retention period, this information should be securely disposed of (these records must be shredded)
Child protection information held in a separate file	25 years after the pupil's date of birth then reviewed	After the retention period, this information should be securely disposed of (these records must be shredded)
Education, training and employment destinations data	At least three years after the pupil has left school	After the retention period, this information should be securely disposed of

Attendance		
Attendance registers	Three years after the date on which the entry was made	After the retention period, this information should be securely disposed of
Correspondence relating to any absence (authorised or unauthorised)	Current academic year plus two years	After the retention period, this information should be securely disposed of
Medical information and administration		
Permission slips	For the duration of the period that medication is given plus one month	After the retention period, this information should be securely disposed of
Medical conditions – ongoing management	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school plus one year	After the retention period, this information should be securely disposed of
Medical incidents that have a behavioural or safeguarding component	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school plus 25 years	After the retention period, this information should be securely disposed of
SEND		
SEND files, reviews and EHC plans, including advice and information to parents regarding educational needs and the accessibility strategy	Pupil's date of birth plus 31 years (the IRMS says this longer retention period is to enable defence in a "failure to provide a sufficient education" case)	After the retention period, this information should be securely disposed of

Curriculum management		
Curriculum returns	Current year plus three years	After the retention period, review and allocate a further retention period or dispose of securely
Timetable	Current year plus one year	After the retention period, review and allocate a further retention period or dispose of securely
Schemes of work	Current year plus one year	After the retention period, review and allocate a further retention period or dispose of securely
Class record books	Current year plus one year	After the retention period, review and allocate a further retention period or dispose of securely. Where appropriate, a sample of books may be retained for impending Ofsted visits.
Mark books	Current year plus one year	After the retention period, review and allocate a further retention period or dispose of securely. Where appropriate, a sample of books may be retained for impending Ofsted visits.
Record of homework set	Current year plus one year	After the retention period, review and allocate a further retention period or dispose of securely

Pupils' work	Where possible, the work should be returned to the pupil at the end of the academic year If this is not possible, the work should be held for the current year plus one year	After the retention period, this information should be securely disposed of
SATs results	Recorded on the pupil's educational record, retained for 25 years after the pupil's date of birth A composite of the whole year's results may be held for the current year plus six years, for comparative purposes	After the retention period, this information should be securely disposed of
Examination papers	Until any appeals/validation process has been completed	After the retention period, this information should be securely disposed of
Published Admission Number (PAN) Reports	Current academic year plus six years	After the retention period, this information should be securely disposed of
Value added and contextual data	Current academic year plus six years	After the retention period, this information should be securely disposed of
Self-evaluation forms (internal moderation)	Current academic year plus one year	After the retention period, this information should be securely disposed of
Self-evaluation forms (external moderation)	Until superseded	After the retention period, this information should be securely disposed of

Extra-curricular activities		
Trip packs – information taken on school trips	Until the end of the visit Where a minor incident occurs, files are added to the core system as appropriate	Shredded upon return to the school
Financial information relating to school trips	Whilst the pupil remains at school plus one year	After the retention period, this information should be securely disposed of
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip or until the end of the academic year (unless a school risk assessment decides the forms are likely to be required for any reason, then they should be retained for 22 years after the pupil's date of birth)	After the retention period, this information should be securely disposed of
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth (permission slips of all pupils on the trip should be held)	After the retention period, this information should be securely disposed of
Walking bus registers	Date of the register being taken plus six years	After the retention period, this information should be securely disposed of If these records are held electronically, all back-up copies should be destroyed at the same time
Educational visitors in school – sharing of personal information	Until the conclusion of the visit plus one month	After the retention period, this information should be securely disposed of

Family liaison officers and home-school liaison assistants		
Day books	Current academic year plus two years	After the retention period, this information should be reviewed and securely disposed of if no longer required
Reports for outside agencies	Duration of the pupil's time at the school	After the retention period, this information should be securely disposed of
Referral forms	Whilst the referral is current	After the retention period, this information should be securely disposed of
Contact data sheets	Current academic year	After the retention period, this information should be reviewed and securely disposed of if contact is no longer active
Contact database entries	Current academic year	After the retention period, this information should be reviewed and securely disposed of if contact is no longer active
Group registers	Current academic year plus two years	After the retention period, this information should be securely disposed of
Catering and free school meal management		
Free school meal registers (where used as a basis for funding)	Current year plus six years	After the retention period, this information should be securely disposed of

School meals registers	Current year plus three years	After the retention period, this information should be securely disposed of
School meals summary sheets	Current year plus three years	After the retention period, this information should be securely disposed of