Our Lady of Light
Catholic Academy Trust

GDPR (General Data Protection Regulation) Policy

The Our Lady of Light Catholic Academy Trust has overarching accountability and governance of four Academies:

- St. Patrick's Catholic College in Thornaby
- St. Patrick's RC Primary School in Thornaby
- Christ the King RC Primary School in Thornaby
- St. Thérèse of Lisieux Catholic Primary School in Ingleby Barwick.

This Policy applies to all schools within the Trust

Policy Dated / Reviewed	March 2018
Adopted / Reviewed by Directors	27 March 2018
Date of next review	April 2019

Contents:

Statement of intent

This policy has been agreed by the Trust's Board for adoption and implementation by each academy and the Trust's Corporate Services Team.

Our Lady of Light Catholic Academy Trust is required to keep and process certain information about its employees and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the DfE, LA, other schools and academies and educational bodies.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the academy complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come 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.

1. Legal framework

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

- 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 Academy 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'

This policy will be implemented in conjunction with the following other Trust/academy policies:

- Photography and Videos at Academy Policy
- E-security Policy
- Freedom of Information Policy
- CCTV Policy

2. 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.

3. 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”.

4. 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 in all of its academies and the Corporate Services Team.

The Trust will provide comprehensive, clear and transparent privacy policies for use in each academy.

Additional internal records of the Trust's processing activities will be maintained and kept up-to-date.

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

Each academy, based on guidance from the Trust, 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.

5. Data protection lead (DPL)

A DPL will be appointed by each academy 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.

Each academy will assign the role of DPL to their Deputy Head Teacher or other senior leader provided that their duties are compatible with the duties of the DPL and do not lead to a conflict of interest. Staff with direct responsibilities for processing personal data on a daily basis cannot act as the DPL and on this basis School Business Managers and other administrative staff will not undertake this role. At the Trust level the Accounting Officer will maintain an oversight of compliance across all of the Trust's academies and provide regular updates to the Board on related issues.

The individuals appointed as DPLs will have professional experience and knowledge of data protection law, particularly that in relation to academies and on this basis all will receive bespoke training in respect of this policy before May 2018. A list of individuals appointed to be DPLs will be provided to the Director of Corporate Services (DFCS) by each academy by 30th April 2018.

DPLs will report to the highest level of management at the academy, which is the headteacher or if requested to the Trust's Accounting Officer, via the DFCS

DPLs will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to DPLs to enable them to meet their GDPR obligations.

6. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under of of 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 one of 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).

7. 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 re-obtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13 (or any other such age as is confirmed by the Government under the Data Protection Bill) 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.

8. 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, the academy 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 DPL.
- 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.

9. 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.

The academy 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.

10. 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 academy will inform them of the rectification where possible.

Where appropriate, the academy 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 academy 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.

11. 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 academy 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.

12. The right to restrict processing

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

In the event that processing is restricted, the academy 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 academy 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 academy has verified the accuracy of the data
- Where an individual has objected to the processing and the academy 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 academy 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 academy 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 academy will inform individuals when a restriction on processing has been lifted.

13. 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 academy will provide the information free of charge.

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

The academy 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 academy will consider whether providing the information would prejudice the rights of any other individual.

The academy 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 academy 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.

14. The right to object

The academy 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 academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the academy 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 academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The academy 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 academy 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 academy will offer a method for individuals to object online.

15. 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 academy 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 academy 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 academy 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.

16. Privacy by design and privacy impact assessments

The academy will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the academy 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 academy's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the academy'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 academy 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 academy will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. 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 DPL supported by the head teacher 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. For administrative purposes this will be done through the Director of Corporate Services on behalf of the Trust’s Accounting Officer.

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 academy 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 DPL
- 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.

18. 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, the academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will only use their personal laptops or computers for academy purposes if they are password protected.

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 academy containing sensitive information are supervised at all times.

The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a termly basis by each academy. 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 Director of Finance & Corporate Services and individual academy DPLs and SBMs are responsible for continuity and recovery measures being in place to ensure the security of protected data.

19. Publication of information

Our Lady of Light Catholic Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

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

Classes of information specified in the publication scheme are made available quickly and easily on request.

Our Trust's academies will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

20. CCTV and photography

The academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The academy 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 six months for security purposes; the SBMs/Premises Leads are responsible for keeping the records secure and allowing access.

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

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

Precautions, as outlined in the **Photography and Videos at Academy Policy**, are taken when publishing photographs of pupils, in print, video or on the academy website.

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

21. Data retention

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the academy 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.

Data retention guidance and periods can be found at Appendix C.

22. 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.

23. Policy review

This policy will be reviewed every 2 years by the Director of Finance & Corporate Services after consultation with the Trust's Board, Accounting Officer and DPLs.

Appendix A – Privacy notice for pupils and their families

Our Lady of Light
Catholic Academy Trust

Privacy Notice for pupils and their families

(How we use pupil information)

The Trust processes pupil and some parent personal data and is the Data Controller of this personal data. The Trust Data Protection Officer is responsible for data protection and can be contacted at St Patrick's Catholic College, Baysdale Road, Thornaby, Stockton-on-Tees TS17 9DE. Tel: (01642) 613327

This notice sets out how the school manages the personal data it uses.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- assessment information
- relevant medical information
- special educational needs information
- exclusions / behavioural information
- CCTV images (We use CCTV to make sure the school site is safe and pupils are safeguarded. Where CCTV is used in private areas such as toilets, it is positioned so as not to compromise privacy)

Why we collect and use this information

We use the pupil data:

- to support pupil learning e.g.
    - personal information to enable accurate pupil records
    - attendance data
    - behavioural information
    - where relevant, details of special educational needs or medical conditions
- to monitor and report on pupil progress e.g.
    - assessment data, including from previous schools
- to provide appropriate pastoral care e.g.
    - attendance or behavioural data may provide an indication of the requirement for pastoral support
    - information about any family circumstances which might affect your child's welfare or happiness.
    - CCTV images may provide evidence of poor behaviour
- to assess the quality of our services e.g.
    - assessment data
- to comply with the law regarding data sharing
- to comply with a legal obligation e.g safeguarding of pupils.
    - CCTV images

We also use personal data of parents/carers to support pupil learning and provide appropriate pastoral care by maintaining up to date contact information to enable efficient communication including in case of emergency.

The lawful bases on which we use this information

The School holds the legal right to collect and use personal data relating to pupils and their families, and may also receive information regarding them from their previous school, LA and/or the Department for Education (DfE).

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the General Data Protection Regulation (GDPR) and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR (from 25 May 2018)
  - consent of the Data Subject e.g use of images and videos of your child
  - the legitimate interest of providing educational services to your child
  - compliance with a legal obligation e.g. safeguarding pupils
  - to protect the vital interests of a Data Subject or another person e.g. promoting the welfare of pupils
- Education Act 1996 e.g. submission of school census returns
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or whether this will need pupil or parental consent, which we will contact you about accordingly.

Storing pupil data

Personal data relating to pupils and their families is stored in line with the Trust's GDPR Data Protection Policy. A copy of which can be found at www.ololcat.org

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. A full list of data retention periods is available in the Trust's GDPR Data Protection Policy.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil attends after leaving us
- our Local Authority (LA)
- the Department for Education (DfE)
- The NHS

The LA, under strict information sharing protocols and policies, may be required to share this information with other public sector partners such as other Local Authorities or local Children's Centres.

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. Data is always shared using secure methods.

The legal basis for sharing data with other schools and the LA is "the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller."

We share pupils' data with the DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the DfE under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services
Pupils aged 13+
Once our pupils reach the age of 13 (or any other such age as is confirmed by the Government under the Data Protection Bill), we also pass pupil information to our LA and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers
- post-16 education and training providers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/pupil once he/she reaches the age defined in GDPR.

The National Pupil Database (NPD)
The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of its data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. Contact the Data Protection Officer to make a request for your personal information, or be given access to your child's educational record**.**

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- data portability
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer at dpo@olocat.org.

Where can you find out more information?
If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit our website www.olocat.org or download our GDPR Data Protection Policy.

Appendix B – Privacy notice for the school workforce

Our Lady of Light Catholic Academy Trust

Privacy Notice

(How we use school workforce information)

Our Lady of Light Catholic Academy Trust will collect and use information about staff in accordance with the data protection principles within the General Data Protection Regulation (GDPR) and is the Data Controller of this personal data.

The Trust Data Protection Officer is responsible for data protection and can be contacted at St Patrick's Catholic College, Baysdale Road, Thornaby, Stockton-on-Tees TS17 9DE, tel: (01642) 613327, email: dpo@olocat.org.

This notice sets out how the school manages the personal data it uses.

This privacy notice outlines what you can expect when the Trust collects your information, if you are a current staff member, or have a temporary or ongoing relationship with the Trust, for example:

- supply teacher engaged through an agency
- volunteer
- parent helper
- contract staff
- Governor or Director

The categories of school workforce information that the Trust collects, processes, holds and shares and the legal basis on which we process this information

Data Held	Reason and Legal Basis for processing
personal information (such as name, address, next of kin, employee or teacher number, national insurance number)	Necessary for the performance of a contract with the dat subject e.g. processing payroll, and necessary for compliance with a legal obligation e.g. making NIC and PA deductions, completion of statutory returns
special categories of data including characteristics information such as gender, age, ethnic group	consent has been obtained from the data subject
contract information (such as start dates, hours worked, post, roles and salary information)	Necessary for the performance of a contract with the dat subject e.g. processing payroll, managing pension records
Bank or building society account details	Necessary for the performance of a contract with the dat subject e.g. making salary payments
work absence information (such as number of absences and reasons)	Necessary for the performance of a contract with the dat subject e.g. paying sick pay
qualifications (and, where relevant, subjects taught)	Necessary to carry out tasks in the public interest e.g. ensuring teachers are appropriately qualified
records concerning performance management and appraisal	Necessary to carry out tasks in the public interest e.g. ensuring teachers and associated staff are providing education and support of an appropriate standard
Correspondence between the member of staff and the Trust	Necessary for the performance of a contract with the dat subject e.g. processing contract changes
Correspondence, such as references, between the Trust and third parties on behalf of a member of staff	consent has been obtained from the data subject
Records of grievances	Necessary for compliance with a legal obligation e.g. compliance with employment law
Investigations into breaches of terms and conditions of employment	Necessary for compliance with a legal obligation e.g. to provide a high standard of education in an appropriate environment and compliance with employment law

Data Held	Legal Basis for processing
Records of disciplinary proceedings	Necessary for compliance with a legal obligation e.g. compliance with employment law
Health and safety records (including accident reports)	Necessary for compliance with a legal obligation e.g. heal and safety regulations
photograph	necessary for compliance with a legal obligation e.g. establishing identity of a person working with children in position of trust
Where appropriate, audio and/or video recording data of staff teaching	Necessary for compliance with a legal obligation e.g. to provide a high standard of education in an appropriate environment
CCTV	Necessary for compliance with a legal obligation e.g safeguarding of pupils. CCTV is also used and to ensure to the school site is safe. Where CCTV is used in private area such as toilets, it is positioned so as not to compromise privacy.

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- perform employment checks e.g. right to work in the UK
- review staff performance
- Monitor absence and sickness records in accordance with HR policy
- enable individuals to be paid
- data collection purposes (e.g. Department of Education School Workforce census)

If staff members fail to provide their personal data, there may be significant consequences. This includes the following:

Employment checks

Failure to provide ample proof of a right to work in the UK will prevent employment with the Trust. Employees found to be working illegally could face prosecution by law enforcement officers.

Salary requirements:

Failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

Special Category personal data

The trust recognises the significance of Special Category personal data and will only process such data if certain conditions are met. These conditions are outlined in guidance from the UK Information Commissioner's Office.

Staff are asked to declare their ethnic origin, and any disabilities at the time of application for a post. These fall within the definition of Special Category data. Consent will be obtained to use this data in the absence of a different legal basis for capturing it e.g. the requirement to submit the School Workforce Census or Gender Pay Gap reporting.

HR files may also contain Special Category personal data in relation to health or sickness, maternity leave or paternity leave. These records will be kept in strict confidence and will not be released to third parties without consent except in extreme cases of emergency i.e. in the vital interests of that data subject.

The lawful basis on which we process this information
The Trust has the legal right to collect and process personal data relating to those we employ, or those otherwise contracted to work in the trust, as specified above.

We also process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Academy Funding Agreement
- Academy's legal framework
- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009

The submission of the School Workforce Census return, including a set of individual staff records, is a statutory requirement on schools and Local Authorities by virtue of regulations SI2007/1264 made under Sections 113 and 114 of the Education Act 2005.

Putting the school census on a statutory basis:

- means that schools may not need to obtain employees' consent to the provision of information
- ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils
- helps to ensure that returns are completed by schools

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

No third parties will be contacted to obtain staff members' personal data without the data subject's consent.

Storing this information
Personal data relating to school workforce is stored in line with the Trust's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. A full list of data retention periods is available in the Trust's GDPR Data Protection Policy.

Who has access to your data?
Access to personnel files is carefully controlled and they may only be seen by the Director of Corporate Services, Headteacher, School Business Manager or other persons, if authorised by the Director of Corporate Services. All staff accessing data are bound by obligations of confidentiality.

Access to personal data held by individual departments will be limited in accordance with that department's operational needs

Where necessary, third parties may be responsible for processing staff members' personal information. Where this is required, the school places data protection requirements on third party processors to ensure data is processed in line staff members' privacy rights. Please see below for details of the applicable third parties.

Who we share this information with and why we share school workforce information

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- Disclosure and Barring Service (DBS)
- Payroll Provider (Xentrall)
- HMRC
- Pension Services (Teachers & Teesside)
- Trade Unions

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and/or our policies allow us to do so.

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our workforce with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. Contact the Data protection Officer to make a request for your personal information.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- data portability
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer at:
St Patrick's Catholic College, Baysdale Road, Thornaby, Stockton-on-Tees TS17 9DE.
tel: (01642) 613327
email: dpo@olocat.org

Further information

If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit our website www.olocat.org or download our GDPR Data Protection Policy.

Appendix C – Data Retention Guidance & Retention Periods

The Trust recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school. This document provides policy guidance through which this effective management can be achieved and audited.

1. **Scope of the Guidance**

This guidance applies to all records created, received or maintained by staff at the school in the course of carrying out its functions.

- Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
- A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research.

2. **Responsibilities**

- The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. Each Headteacher has overall responsibility for this policy.
- The person responsible for records management in the school, usually the SBM, will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.
- Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's records management guidelines.

3. **Relationship with Existing Policies**

This guidance has been drawn up within the context of:

- Freedom of Information Policy.
- Other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

4. Safe Disposal of Records

Where records have been identified for destruction they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information, should be shredded before disposal using a cross cut shredder. Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in the dustbin or a skip.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier).
- File title (or brief description) and number of files.
- The name of the authorising officer and the date action taken.

This should be kept in an Excel spreadsheet or similar suitable format.

5. Transfer of Information

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

6. Academy Closures

Should an academy close there will be records which will need to be stored until they work out their statutory retention periods. It is the responsibility of the Trust to manage these records until they have reached the end of their administrative life and to arrange for their disposal when appropriate. There may be a number of different reasons why a school has closed and this may affect where the records need to be stored.

- If the school has been closed and the site is being sold or reallocated to other use then the Trust should take responsibility for the records from the date the academy closes.

- If two schools have merged onto one site and then function as one school, it is sensible to retain all the records relating to the two schools on the one site.

7. Retention Guidelines

The following retention guidelines have been issued by the Management Society of Great Britain 'Retention Guidelines for Schools'. Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be 'normal processing' under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

Child Protection					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Child Protection files	Yes	Education Act 2002, related guidance "Safeguarding Children in Education", September 2004	Date of leaving + 25 years	Shred	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (the information does not need to be sent to a university) Where a child is removed from roll to be educated at home, the file should be copied to the Local Authority.
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Shred	The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60: "Record Keeping 5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future DBS Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."

Governors					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Principal set Minutes (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives
Inspection copies	No		Date of meeting + 3 years	SHRED	
Agendas	No		Date of meeting	SHRED	
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives
Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives
Instruments of Government	No		Permanent	Retain in school	Transfer to Archives when the school has closed
Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives
Action Plans	No		Date of action plan + 3 years	SHRED	It may be appropriate to offer to the Archives
Policy documents	No		Expiry of policy	Retain in school whilst policy is operational	Transfer to Archives
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SHRED routine complaints	
Annual Reports required by the Department for Education and Skills	No		Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	Transfer to Archives
Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years	Transfer to Archives

Management					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Log Books	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Minutes of the Senior Management Team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to the Archives
Reports made by the head teacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to the Archives
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	SHRED	
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Date of correspondence + 3 years	SHRED	
Professional development plans	Yes		Closure + 6 years	SHRED	
School development plans	No		Closure + 6 years	Review	Offer to the Archives
Admissions – if the admission is successful	Yes		DOB of the pupil + 25 years	SHRED	
Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SHRED	
Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SHRED	

Pupils					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Attendance registers	Yes		Date of register + 3 years	SHRED	
Pupil record cards	Yes				
Secondary		Limitation Act 1980	DOB of the pupil + 25 years	SHRED	
Pupil files	Yes				
Secondary		Limitation Act 1980	DOB of the pupil + 25 years	SHRED	
Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years	SHRED	
Absence books			Current year + 6 years	SHRED	
Examination results	Yes				
Public examination results	No		Year of examinations + 6 years	SHRED	Unclaimed certificates returned to Exam Board
Internal examination results	Yes		Current year + 5 years	SHRED	

Pupils				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SHRED
Statement maintained under The Education Act 1996 - Section 324	Yes	SEN and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending
Proposed statement or amended statement	Yes	SEN and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending
Advice and information to parents regarding educational needs	Yes	SEN and Disability Act 2001 Section 1	Closure + 12 years	SHRED unless legal action is pending
Accessibility Strategy	Yes	SEN and Disability Act 2001 Section 1	Closure + 12 years	SHRED unless legal action is pending
Children's SEN Files	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SHRED unless legal action is pending
Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SHRED
Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SHRED
Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	3 part supplement to the H&S of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	SHRED

Curriculum				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Curriculum development	No		Current year + 6 years	SHRED
Curriculum returns	No		Current year + 3 years	SHRED
School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
Examination results	Yes		Current year + 6 years	SHRED
SATS records	Yes		Current year + 6 years	SHRED
PAN reports	Yes		Current year + 6 years	SHRED
Value added records	Yes		Current year + 6 years	SHRED

Staff records				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SHRED
Staff Personal files	Yes		Termination + 7 years	SHRED
Interview notes and recruitment records	Yes		Date of interview + 6 months	SHRED
Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months	SHRED
Disciplinary proceedings:	Yes	Where the warning relates to child protection issues then retain until the person's normal retirement age, or 10 years from the date of the allegation, whichever is the longer If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.		
• oral warning			Date of warning + 6 months	SHRED
• written warning – level one			Date of warning + 6 months	SHRED
• written warning – level two			Date of warning + 12 months	SHRED
• final warning			Date of warning + 18 months	SHRED
• case not found			If child protection related then retain until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer. Otherwise shred immediately at the conclusion of the case	SHRED
Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SHRED
Annual appraisal/assessment records	No		Current year + 5 years	SHRED
Salary cards	Yes		Last date of employment + 85 years	SHRED
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, + 3yrs	SHRED
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SHRED
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file.	

Health and Safety				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SHRED
Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
Adults	Yes		Date of incident + 7 years	SHRED
Children	Yes		DOB of child + 25 years	SHRED
COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	SHRED
Incident reports	Yes		Current year + 20 years	SHRED
Policy Statements			Date of expiry + 1 year	SHRED
Risk Assessments			Current year + 3 years	SHRED
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SHRED
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SHRED
Fire Precautions log books			Current year + 6 years	SHRED

Administrative					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Employer's Liability certificate			Closure of the school + 40 years	SHRED	
Inventories of equipment and furniture			Current year + 6 years	SHRED	
General file series			Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives
School brochure or prospectus			Current year + 3 years		Transfer to Archives
Circulars (staff/parents/pupils)			Current year + 1 year	SHRED	
Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives
Visitors' book			Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives
PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives

Finance					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Annual Accounts		Financial Regulations	Current year + 6 years	Offer to the Archives	Annual Accounts
Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Contracts under seal			Contract completion date + 12 years	SHRED	
Contracts under signature			Contract completion date + 6 years	SHRED	
Contracts monitoring records			Current year + 2 years	SHRED	

Finance					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Copy orders			Current year + 2 years	SHRED	
Budget reports, budget monitoring etc.			Current year + 3 years	SHRED	
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SHRED	
Annual Budget and background papers			Current year + 6 years	SHRED	
Order books and requisitions			Current year + 6 years	SHRED	
Delivery Documentation			Current year + 6 years	SHRED	
Debtors' Records		Limitation Act 1980	Current year + 6 years	SHRED	
School Fund – Cheque books			Current year + 3 years	SHRED	
School Fund – Paying in books			Current year + 6 years then review	SHRED	
School Fund – Ledger			Current year + 6 years then review	SHRED	
School Fund – Invoices			Current year + 6 years then review	SHRED	
School Fund – Receipts			Current year + 6 years	SHRED	
School Fund – Bank statements			Current year + 6 years then review	SHRED	
School Fund – School Journey books			Current year + 6 years then review	SHRED	
Applications for free school meals, travel, uniforms etc			Whilst child at school	SHRED	
Student grant applications			Current year + 3 years	SHRED	
Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SHRED	
Petty cash books		Financial Regulations	Current year + 6 years	SHRED	

Property					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Title Deeds			Permanent	Permanent these should follow the property unless the property has been registered at the Land Registry	Offer to Archives if the deeds are no longer needed
Plans			Permanent	Retain in school whilst operational	Offer to Archives
Maintenance and contractors		Financial Regulations	Current year + 6 years	SHRED	
Leases			Expiry of lease + 6 years	SHRED	
Lettings			Current year + 3 years	SHRED	
Burglary, theft and vandalism report forms			Current year + 6 years	SHRED	
Maintenance log books			Last entry + 10 years	SHRED	
Contractors' Reports			Current year + 6 years	SHRED	

Local Authority					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SHRED	
Attendance returns	Yes		Current year + 1 year	SHRED	
Circulars from LA			Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archive

Department for Education					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
HMI reports			These do not need to be kept any longer		Transfer to Archives
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives
Returns			Current year + 6 years	SHRED	
Circulars from Department for Education			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives

Connexions / Prospects					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Service level agreements			Until superseded	SHRED	
Work Experience agreement			DOB of child + 18 years	SHRED	

School Meals					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**	
Dinner Register			Current year + 3 years	SHRED	
School Meals Summary Sheets			Current year + 3 years	SHRED	

Other Records - Administration			
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**
Financial Records			
Financial records – accounts, statements, invoices, petty cash etc	No		Current year + 6 years
Insurance			
Insurance policies – Employers Liability	No	Employers Liability Financial Regulations	The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy
Claims made against insurance policies – damage to property	Yes		Case concluded + 3 years
Claims made against insurance policies – personal injury	Yes		Case concluded + 6 years
Human Resources			
Personal Files - records relating to an individual's employment history	Yes**		Termination + 6 years then review
Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months
Staff training records – general	Yes		Current year + 2 years
Training (proof of completion such as certificates, awards, exam results)	Yes		Last action + 7 years
Premises files (relating to maintenance)	No		Cessation of use of building + 7 years then review
Risk Assessments	No		Current year + 3 years
Staff training records – general	Yes		Current year + 2 years
Training (proof of completion such as certificates, awards, exam results)	Yes		Last action + 7 years
Premises and Health and Safety			
Premises files (relating to maintenance)	New		Cessation of use of building + 7 years then review
Risk Assessments	New		Current year + 3 years

**For Data Protection purposes the following information should be kept on the file for the following periods:

All documentation on the personal file — Duration of employment
Pre-employment and vetting information — Start date + 6 months
Records relating to accident or injury at work — Minimum of 12 years
Annual appraisal/assessment records — Minimum of 5 years
Records relating to disciplinary matters (kept on personal files)

- oral warning — 6 months
- first level warning — 6 months
- second level warning — 12 months
- final warning — 18 months