“Excellent Learning, Teaching and Leadership for All”

Data Protection Policy (GDPR)

1. Statement of intent

Windsor Learning Partnership 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) and the expected provisions of the Data Protection Act 2018 as set out in the Data Protection Bill.

The Trust may, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority (LA), other schools and educational bodies, and other agencies such as social services.

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

Organisational methods for keeping data secure are imperative, and Windsor Learning Partnership believes that it is good practice to have clear practical policies.

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

2. Legal framework

2.1 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 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
- The Protection of Freedoms Act 2012

2.2 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'
- Information Commissioner's Office code of practice for the use of surveillance cameras and personal information.

3. Applicable data

3.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living, natural person including information such as an online identifier, such as 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.

3.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation and data concerning health matters.

4. Principles

4.1 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.

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

5. Accountability

5.1 Windsor Learning Partnership will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5.2 The Trust will provide comprehensive, clear and transparent privacy policies.

5.3 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.

5.4 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

5.5 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.
- Continuously creating and improving security features.

5.6 Data protection impact assessments will be used, where the Trust brings in new initiatives or systems with high risk processing.

6. Roles and Responsibilities

6.1 The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with its obligations under all relevant data protection obligations.

6.2 The Headteacher

Day-to-day responsibilities of acting as the representative of the data controller rest with the Headteacher and the Chief Operating Officer of the Trust. Each school will also act as the Data Controllers representatives under the delegation of the Headteacher. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee the implementation of the policy.

6.3 The Data Controller

The Data Controller is Windsor Learning Partnership Board of Trustees. Windsor Learning Partnership pays the data protection fee required by the Information Commissioners Office.

6.4 The Data Protection Officer (DPO)

The Trust's DPO is:
Jennifer Shaw, Data Protection Officer, Senior Information Governance Officer, Law and Governance Service, Royal Borough of Windsor & Maidenhead, St. Ives Road, Maidenhead, SL6 1RF, Tel: 01628 796675.

The role of the DPO will be to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust'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.
- The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to Trusts.
- The DPO will report to the highest level of management at the Trust, which is the headteacher.
- The DPO will operate independently and will not be dismissed or penalised for performing their task.
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

- The DPO is a point of contact for individual's whose data the Trust processes, and for the ICO.

6.5 All Staff

- All Staff are responsible for:
- Ensuring that they collect and store any personal data in accordance with this policy;
- Inform the Trust of any changes to their own personal data;
- Reporting to the Headteacher if they have concerns that this policy is not being followed;
- Reporting any data breaches immediately as the DPO has to report to the ICO within 72 hours;
- Reporting if they are engaging in a new activity that may affect the privacy rights of individuals;
- Requesting guidance from the Trust Chief Operating Officer on sharing data with third parties and where necessary the appropriate Information Sharing Agreement (ISA) completed;
- Request authority from a member of the Senior Leadership team and the IT Manager (if applicable) before engaging 3rd party software or services.

7 Lawful processing

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

7.2 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.
  - Public Task, in that 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.

7.3 Special categories of personal 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 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).

8 Consent

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

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

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

8.4 The Trust 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. Advice should be sought from the Trust's DPO;

8.5 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.

8.6 Consent can be withdrawn by the individual at any time where the information provided is voluntary.

8.7 The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

9 The right to be informed- Privacy Notices

9.1 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.

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

9.3 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.
    - Object
- The Trust does not use automated decision-making.

9.4 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 and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

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

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

9.7 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.

10 The right of access

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

10.2 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.

10.3 The Trust will verify the identity of the person making the request before any information is supplied.

10.4 When a subject access request is made by a parent and the child is over 13 years old the child's permission is required for the disclosure of the information to the parent.

10.5 A copy of the information will be supplied to the individual free of charge; however, the Trust may charge to comply with requests for further copies of the same information. This charge will be 10p per copy.

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

10.7 Where a request is manifestly unfounded, excessive or repetitive, we will refer to the DPO for guidance on refusal or charging.

10.8 All fees will be based on the administrative cost of providing the information – staff time cannot be charged for.

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

10.10 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.

10.11 Where a request is manifestly unfounded or excessive, the Trust 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.

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

See Appendix 1 for the Subject Access Request Procedure.

11. Other data protection rights of the individual

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

- Withdraw their consent to processing at any time where the processing relies on consent
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

12. Privacy by design and privacy impact assessments

12.1 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 when it brings new initiatives or systems and there is high risk processing.

12.2 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.

12.3 DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Windsor Learning Partnership's reputation which might otherwise occur.

12.4 A DPIA will be used when using or introducing new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

12.5 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

12.6 The Trust 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

12.7 Where a DPIA indicates high risk data processing, the Trust will consult its DPO and the ICO if necessary to seek its opinion as to whether the processing operation complies with the GDPR.

12.8 The DPIA will consider the benefits vs the impact on individual privacy and will consider if the risk can be mitigated or are there other ways to do the same thing.

13 Data breaches

13.1 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.

13.2 The headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach and how to report it to the appropriate person in Trust as part of their continuous development training.

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

13.4 All personal data breaches need to be reported to the Trusts DPO (dpa@rbwm.gov.uk)

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

13.6 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.

13.7 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.

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

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

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

13.11 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

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

See Appendix 2 for the Personal data breach procedure

14. Data security

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

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

14.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up in separate buildings.

14.4 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.

14.5 Removable storage and portable devices used to access personal data will not be used to hold personal information unless they are password-protected and fully encrypted.

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

14.7 Staff and governors will not use their personal laptops or computers for Trust purposes.

14.8 All members of staff are provided with their own secure login and password and are prompted to change this every three months.

14.9 Staff who access emails on personal mobile devices must ensure their device security passcodes are alphanumeric.

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

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

14.12 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 Trust premises accepts full responsibility for the security of the data.

14.13 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;
- The identity of the recipient has been verified.

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

14.15 The physical security of the Trust'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.

14.16 Windsor Learning Partnership takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

14.17 Each Head teacher is responsible for ensuring recovery measures are in place to ensure the security of protected data.

15. Publication of information

15.1 Windsor Learning Partnership publishes a publication scheme on its website as part of the its Freedom of Information Policy outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

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

15.3 Windsor Learning Partnership will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

16. CCTV, photography and video

We use CCTV in various locations around the Trust site to ensure it remains safe.

We do not need to ask individuals permission to use CCTV, but cameras are clearly visible and there are signs at entrances to the site stating that CCTV is in use.

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

16.2 The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via, letters, email and privacy notices.

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

16.4 All CCTV footage will be kept for 32 days for security purposes; the Headteacher is responsible for keeping the records secure and allowing access.

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

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

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

17 Biometric recognition systems

17.1 Where we use pupils' biometric data as part of an automated biometric recognition system (cashless catering) we will comply with the requirements of the Protection of Freedoms Act 2012. NB: Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18

17.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we process any biometric data from their child.

17.3 Parents/carers and students can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

17.4 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

17.5 Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

18 Data retention

18.1 Data will retained in line with the Trusts retention guidelines and can be found in appendix 3.

18.2 Unrequired data will be deleted as soon as practicable.

18.3 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.

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

19 DBS data

19.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

19.2 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.

20. Communication of policy

20.1 This policy will be published on the Trust website and the staff information drive.

21. Evidence of implementation

21.1 The Finance & Resources Committee of the Governing Body will review any recommendations for action made by the DPO.

22 Review of Policy

22.1 This policy shall be reviewed every two years by the Audit and Risk committee.

Appendix 1 – Subject Access Request Procedure (SAR)

General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 as set out in the Data Protection Bill extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the Trust's policy is that:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.

- All children aged 13 and over have their own information rights provided they are Fraser competent (they are considered mature enough to understand the data). Any subject access request made from a parent of a child aged 13 and over will only be processed if the Trust have consent from the child to disclose the information to the parent and that the Trust are satisfied the consent was freely given.

Processing Subject Access Requests

Requests for access must be made in writing. In many cases a letter to the Headteacher will be sufficient to identify the information required.

Provided that there is sufficient information to process the request, a record will be made showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record). Where the request is made by a parent or a person with parental responsibility of a student over 13 years of old the consent of the student must also be provided. In this case the request deadline will be one month from the date of receipt of the consent of the student.

Requests from Carers who do not have parental responsibility will be considered by the Headteacher on an individual basis who will obtain legal advice if required on how to make a legal disclosure.

The Headteacher must be confident of the identity of the individual making the request. If not, this can be checked by the request to provide photographic ID such as passport or photo driving licence.

All files must be reviewed before any disclosure takes place. The data subject is only entitled to information about them. Any other individuals mentioned within the records must be redacted. The redaction may entail removal of information or anonymisation/pseudonymisation of the documents.

Where information has been provided to Windsor Learning Partnership by a third party, for example, the local authority, the police, a health care professional or another school, but is held on the Trust's file it is good practice to seek the consent of the third party before disclosing information. If the third party does not consent it may be necessary to seek additional advice from the DPO.

The applicant should be told the data that the Trust holds, be given a copy of the data, and be told the purposes for which it is processed and whether it has been shared with any other party. The Headteacher must at all times consider the welfare of the child.

Where particular data in a document cannot be disclosed a permanent copy should be made and the data obscured and re-copied. A full copy of the document before obscuring and the altered document should be retained together with the reason why the document was altered, so that in the event of a complaint there is an audit trail of what was done and why.

Data refers to paper records and all records held on computer or other mediums. A report of data held on the Trust information database, known as a personal data output report, should be requested via the Trusts Chief Operating Officer.

If the applicant wishes to make a complaint about how their SAR has been dealt with they should write to the Chief Operating Officer for the Trust.

Appendix 2: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately report the breach directly to:
    - The Headteacher of the relevant school.
    - The Schools DPO: dpa@rbwm.gov.uk 01628 796945
- The DPO will be informed.
- The report will be investigated and it will be determined whether a breach has occurred. To decide, consideration will be given as to whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Chair of Governors of the relevant school will be informed.
- The DPO and Data Controllers will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

    If it's likely that there will be a significant risk to people's rights and freedoms, the DPO must notify the ICO.
- The Trust will document the decision where it has not been referred to the ICO. The DPO will document the process for those referred to the ICO. Decisions will be recorded on the Trusts GDPRiS system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Trust will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Trusts GDPRiS system.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Special categories of personal data being disclosed via email (including safeguarding records)

- information containing special categories of personal data must be sent as a password protected document;

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error;
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error;
- If the sender is unavailable or cannot recall the email for any reason, the Trust will ask the ICT department to recall it. This relates to internally sent mail only;
- In any cases where the recall is unsuccessful, the Trust will contact the relevant un-authorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way;
- The Trust will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request;
- The Trust will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Details of pupil premium interventions for named children being published on the Trust website

- If personal data is accidentally made available through public websites, the owner of the webpage must take immediate steps to ensure the data is removed by contacting the website owner or administrator
- The member of staff aware of the breach must alert the DPO as soon as they become aware of it
- The Trust will carry out an internet search to check that the information has not been further disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Non-anonymised pupil exam results or staff pay information being shared with trustees/ governors

- All papers circulated to trustees and governors will be checked by the writer and the Clerk to Governors to ensure that no personal data or special category data is included in the papers
- If personal or special category data is shared with governors, the trustee/ governor/ member of staff who becomes aware of the data breach must alert the DPO as soon as they become aware of it
- The Trust must contact all recipients of the information and ask them to delete the information and not share, publish, save or replicate it in any way
- The Trust will ensure a written response is received from all the individuals who received the data, confirming that they have complied with this request
- The Trust will ask the writer of the papers to re-issue them with the personal data or special category data removed.

A Trust laptop or USB containing non-encrypted sensitive personal data being lost, stolen or hacked

- The member of staff aware of the breach must alert the DPO as soon as they become aware of it
- The Trust must alert the police of the loss if appropriate and take all possible steps available to them to retrieve the data.
- The Trust, where possible, will enable remote blocking.
- The Trust, to establish whereabouts of the bit locker.
- The Trust must make the owner of the personal data, if any is lost, stolen or hacked, aware of the loss of the data.
- The Trust will carry out an internet search to check that the information has not been disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 3 – Retention Guidelines

A. Summary of areas within these guidelines:

Ref	Area
1	Management of the School
2	Human Resources
3	Financial Management of the School
4	Property Management
5	Pupil Management
6	Curriculum Management
7	Extra-Curricular Activities
8	Central Government and Local Authority

A. Aims

These guidelines have been produced based on the "Information Management Toolkit for Schools" (IMTIS) dated 1 February 2016 and developed and published by the Information Record Management Society ("IRMS").

These guidelines have been produced in accordance with the guidance produced by the DFE in April 2018 in the "GDPR Toolkit for Schools" and is in accordance with the Data Protection rules and Freedom of Information Act (2000) legislation.

This is a guideline developed to enable school staff to carry out the retention and destruction of school records and information.

B. Safe Destruction of Data

(i) Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle as per the data protection rules (updated for GDPR) states that:

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"

In each school, the leadership must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are retained.

The school review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the school for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the records management policy within the school.

(ii) Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

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 with the regular waste or a skip unless there is no other alternative.

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.

1. Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		
	Principal Set (signed)		PERMANENT	If the school is unable to store these then they should be offered to the LA Archives Service
	Inspection Copies		Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff	Reports should be kept for a minimum of 6 years. However, If the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' (if applicable) meeting held under section 33 of the Education Act 2002	No	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1.1 Governing Body (continued…)				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.1.5	Instruments of Government including Articles of Association	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No	Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No	Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes	Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No	Date proposal accepted or declined + 3 years	SECURE DISPOSAL

1.2 Head Teacher and Senior Management Team				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff	Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the LA Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff	Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff	Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff	Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff	Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes	Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No	Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
1.3.5	Admissions – Secondary Schools – Casual	Yes	Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Current year + 1 year	SECURE DISPOSAL
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes		
	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions		Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
1.4.1	General file series	No	Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No	Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No	Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes	Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No	Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes	Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	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	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.2 Operational Staff Management				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.2.1	Staff Personal File	Yes	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes	Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes	Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes		
	oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1		Date of warning + 6 months	
	written warning – level 2		Date of warning + 12 months	
	final warning		Date of warning + 18 months	
	case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.4.1	Health and Safety Policy Statements	No	Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No	Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	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	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes		
	Adults		Date of the incident + 6 years	SECURE DISPOSAL
	Children		DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No	Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No	Current year + 6 years	SECURE DISPOSAL

2.5 Payroll and Pensions				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
2.5.1	Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	SECURE DISPOSAL

3 Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals

3.1 Risk Management and Insurance				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.1.1	Employer's Liability Insurance Certificate	No	Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.2.1	Inventories of furniture and equipment	No	Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No	Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.3.1	Annual Accounts	No	Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No	Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes	Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No	Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking ofmonies	No	Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No	Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.4.1	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No	Current year + 2 years	SECURE DISPOSAL

3.5 School Fund				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.5.1	School Fund - Cheque books	No	Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No	Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No	Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No	Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No	Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No	Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No	Current year + 6 years	SECURE DISPOSAL

3.6 School Meals				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
3.6.1	Free School Meals Registers	Yes	Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes	Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No	Current year + 3 years	SECURE DISPOSAL

4 Property Management

This section covers the management of buildings and property.

4.1 Property Management				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
4.1.1	Title deeds of properties belonging to the school	No	PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No	These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No	Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No	Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
4.2.1	All records relating to the maintenance of the school carried out by contractors	No	Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No	Current year + 6 years	SECURE DISPOSAL

5 Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above

5.1 Pupil's Educational Record				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.1.1	Pupil's Educational Record	Yes		
	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [1]
	Secondary		Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes		
	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal		This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files		DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

[1] This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority

5.2 Attendance				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.2.1	Attendance Registers	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6 Curriculum Management

6.1 Statistics and Management Information				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
6.1.1	Curriculum returns	No	Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes	Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes		
	Results		The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes	Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes	Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes	Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
6.2.1	Schemes of Work	No	Current year + 1 year	Review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No	Current year + 1 year	
6.2.3	Class Record Books	No	Current year + 1 year	
6.2.4	Mark Books	No	Current year + 1 year	
6.2.5	Record homework set	No	Current year + 1 year	
6.2.6	Pupils' Work	No	Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7. Extra Curriculum Management

7.1 Educational Visits outside the Classroom				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes	Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
7.2.1	Walking Bus Registers	Yes	Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
7.3.1	Day Books	Yes	Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes	Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes	While the referral is current	
7.3.4	Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes	Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes	Current year + 2 years	

8. Central Government and Local Authority

8.1 Local Authority				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.1.1	Secondary Transfer Sheets (Primary)	Yes	Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes	Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No	Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No	Operational use	SECURE DISPOSAL

8.2 Central Government				
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.2.1	OFSTED reports and papers	No	Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No	Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No	Operational use	SECURE DISPOSAL