Mayville Primary School
Data Protection and Privacy Policy

Approved by:	Audit and Resources Committee	**Date:**	6 October 2021
Last reviewed on:	October 2021		
Next review due by:	October 2022		

1. STATEMENT OF INTENT

1.1 Mayville Primary School is required to keep and process certain information about its staff and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the local authority, other schools, educational bodies, social services and possibly the police/solicitors.

1.2 This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Mayville Primary School believes that it is good practice to keep clear practical policies, supported by written procedures.

1.3 To ensure the full compliance with GDPR, all staff receive data protection training and/or data protection information.

2. LEGAL FRAMEWORK

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

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

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)'
- DfE Data protection: a toolkit for schools (April 2018).

2.3 This policy will be implemented in conjunction with the following other school policies:

- E-safety Policy
- Teaching and Learning Policy
- Freedom of Information Policy.

2.4 Mayville Primary School is categorised as a data controller and is registered with the Information Commissioner's Office (ICO) – Registration Number: 10035844.

3. APPLICABLE DATA

3.1 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, for instance 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', which are the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. PRINCIPLES

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

a. Processed lawfully, fairly and in a transparent manner in relation to individuals.
b. 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 incompatible with the initial purposes.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. 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.
e. 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.
f. 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.

5. ACCOUNTABILITY

5.1 Mayville Primary School 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 school will provide comprehensive, clear and transparent privacy notices.

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 for processing activities (Data Export Record Sheet) includes the following:

a. Data ID number
b. Date of processing
c. Name and department of internal requester
d. Description of the data for export
e. Reason for the export of personal data
f. Receiving body and contact details
g. Description of technical and organisational security measures

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

a. Data minimisation
b. Pseudonymisation *(can be used as an alternative to encryption, example: Initials used to replace staff/students full names i.e. John Smith replaced by JS)*
c. *Transparency*
d. Continuously creating and improving security features.

5.6 Data protection impact assessments will be used where appropriate.

6. DATA PROTECTION OFFICER (DPO)

6.1 The school's trustees have appointed a DPO, in order to:

a. Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
b. Monitor the school'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.
c. The DPO is responsible for maintaining the Data Protection policy and associated documents. The DPO submits the policy to the trustees for review, on an annual basis.

6.2 The DPO has proficient experience and knowledge of data protection law, particularly that in relation to schools. The DPO will report to the highest level of management at the school, which is the chair of trustees and the headteacher.

7. LAWFUL PROCESSING

7.1 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 the following conditions:

a. The consent of the data subject has been obtained
b. Compliance with a legal obligation
c. The performance of a task carried out in the interest of the curriculum or in the exercise of official authority vested in the school
d. For the performance of a contract with the data subject or to take steps to enter into a contract
e. Protecting the vital interests of a data subject or another person
f. For the purposes of legitimate interests pursued by the school as the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.2 Sensitive data will only be processed under the following conditions:

a. Explicit consent of the data subject
b. 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.

c. Processing relates to personal data manifestly made public by the data subject.

7.3 Processing is necessary for:

a. Carrying out obligations under employment, social security or social protection law, or a collective agreement.
b. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
c. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
d. 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.
e. 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 a lawful basis or a contract with a health professional.
f. Reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
g. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with GDPR article 89(1).

8. CONSENT

8.1 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.

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

8.3 The school 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.

8.4 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR. However, once acceptable consent has been obtained under the DPA, it will not be reobtained.

8.5 Consent can be withdrawn by the individual at any time.

8.6 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. When processing data online, parental consent is not required when the child reaches the age of 13.

9. THE RIGHT TO BE INFORMED

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 school 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:

a. The identity and contact details of the school (controller), and where applicable, the controller's representative and the DPO.
b. The purpose of, and the legal basis for, processing the data.
c. The legitimate interests of the controller or third party.
d. Any recipient or categories of recipients of the personal data.
e. Details of transfers to third countries and the safeguards in place.
f. The retention period of criteria used to determine the retention period.

9.4 The existence of the data subject's rights, including the right to:

a. Withdraw consent at any time.
b. Lodge a complaint with a supervisory authority.

9.5 The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

9.6 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.

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

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

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

Privacy Notices are attached at Appendix 1.

10. THE RIGHT OF ACCESS

10.1 Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data. The school will verify the identity of the person making the request before any information is supplied or viewed.

10.2 Personal data can be viewed by the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for paper copies of the information.

10.3 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.

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

10.5 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.

10.6 Where a request is manifestly unfounded or excessive, the school 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.

10.7 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.
Subject Access Request (SAR) form is attached at Appendix 2.

11. THE RIGHT TO RECTIFICATION

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

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

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

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

12. THE RIGHT TO ERASURE

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

12.2 Individuals have the right to erasure in the following circumstances:

a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
b. When the individual withdraws their consent.
c. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
d. The personal data was unlawfully processed.

e. The personal data is required to be erased in order to comply with a legal obligation.
f. The personal data is processed in relation to the offer of information society services to a child.

12.3 The school 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.

12.4 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.

12.5 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.

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

13. THE RIGHT TO RESTRICT PROCESSING

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

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

13.2 If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The school will inform individuals when a restriction on processing has been lifted.

14. THE RIGHT TO DATA PORTABILITY

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

14.2 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:

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

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

14.4 The school will provide the information free of charge.

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

14.6 Mayville Primary School is not required to adopt or maintain processing systems, which are technically compatible with other organisations.

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

14.8 The school will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

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

15. THE RIGHT TO OBJECT

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

15.2 Individuals have the right to object to the following:

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

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

a. An individual's grounds for objecting must relate to his or her particular situation.

b. The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4 Where personal data is processed for direct marketing purposes:

a. The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
b. The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

16. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

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

16.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused Mayville Primary's reputation, which might otherwise occur. A DPIA will be used 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.

16.3 High risk processing includes, but is not limited to, the following:
a. Systematic and extensive processing activities, such as profiling.
b. Large scale processing of special categories of data or personal data

16.4 The school will ensure that all DPIAs include the following information:
a. A description of the processing operations and the purposes
b. An assessment of the necessity and proportionality of the processing in relation to the purpose
c. An outline of the risks to individuals
d. The measures implemented in order to address risk.

16.5 Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.
DPIA form is attached at Appendix 5.

17. DATA BREACHES

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

17.2 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 school becoming aware of it.

17.3 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.

17.4 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school 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.

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

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

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

a. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
b. The name and contact details of the DPO
c. An explanation of the likely consequences of the personal data breach
d. A description of the proposed measures to be taken to deal with the personal data breach
e. Where appropriate, a description of the measures taken to mitigate any possible adverse effects
f. Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

Data breach reporting form is attached at Appendix 3.

18. DATA SECURITY

18.1 No personal data is to be taken offsite, unless approved by the headteacher.

18.2 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. If no longer required, paper records are to be put in to a 'white confidential waste sack' for onward secure destruction or shredded.

18.3 Hard drives and network drives are protected using New Technology File System (NTFS) permissions. 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.

18.4 USB Memory sticks are not be used to hold personal information unless they are password-protected and fully encrypted. Only school sanctioned encrypted memory stick can be used. All electronic devices are to be password-protected to protect the information on the device in case of theft. PC's will be read only enabled, data cannot be uploaded to USB Memory Sticks.

18.5 Dictaphones which hold confidential meeting minutes, are securely controlled by the admin team, the recordings are deleted after use.

18.6 The school has a remote gateway and Freedom to Roam, school staff can access school data offsite by using this secure access method. Freedom to Roam LGFL must only be accessed via Office 365 and no data is to be saved to the users' personal device.

18.7 Staff are provided with their own secure login and password on their contract start date, and every computer regularly prompts users to change their password.

18.8 Emails containing sensitive or confidential information are to be password-protected and a log is maintained recording the data control.

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

18.10 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 School premises accepts full responsibility for the security of the data. Staff are prohibited from transporting paper copies of personal data via public transport (encrypted USB sticks can be used to transport data via public transport).

18.11 School trips – For 'offsite activities student emergency information' the trip organiser is to save the information in a pdf format and upload to a Kindle device (supplied by the IT dept). Paper copies are not to be taken offsite.

18.12 Before sharing data, all staff members will ensure:

a. They are allowed to share it (approval required from the headteacher).

b. That adequate security is in place to protect it.

c. Who will receive it, are entitled to receive the information or are disclosed under our Privacy Notice.

d. A data sharing log is to be maintained by the data administrator.

18.13 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place. Mayville Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.14 The network manager is responsible for continuity and recovery measures that are in place to ensure the security of protected digital data, which includes disabling access to electronic data when a staff member terminates their employment with the school.

19. PUBLICATION OF INFORMATION

19.1 Mayville Primary School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

a. Policies and procedures

b. Reports

c. Financial information.

19.2 Classes of information specified in the publication scheme are made available quickly and easily on request. (School name here) will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the school website, staff are considerate of any metadata or deletions, which could be accessed in documents and images on the site.

20. CCTV AND PHOTOGRAPHY

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

20.2 The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via signage. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.3 All CCTV footage will be kept for 30 days for security purposes; the network manager is responsible for keeping the records secure and allowing access.

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

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

20.6 On an annual basis, the school commissions a professional photographer to take student and staff photographs for school use. The professional photographer also offers parents/guardians to purchase a photograph of their child, this is a private arrangement between the photographer and the parent/guardian.

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

21. DATA RETENTION AND DISPOSAL

21.1 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 school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. The school has adopted the HCC 'Retention Schedule for Schools', which has been created to assist schools to manage their information in line with the current legislative framework.

21.2 Paper documents are disposed of by using the provided 'crosscut' shredders.

22. DISCLOSURE AND BARRING SERVICE (DBS) DATA

22.1 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.

22.2 Roles in schools are legally eligible for DBS checks and the DBS have published a 'Consent Privacy Policy' to ensure individuals are fully informed of the use of their personal data; their rights and that the school via Waltham Forest meets the necessary requirements when submitting DBS checks. The 'DBS Consent Privacy Policy' explains customer rights for their data protection:

22.3 Visit: https://www.gov.uk/government/publications/consent-privacy-policy

23. RESPONSIBILITIES

23.1 All staff within the school are responsible for protecting and ensuring the security of the personal data to which they have access and/or process. Managers and staff are responsible for ensuring that all information in their direct work area is managed appropriately, in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

23.2 The school will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.

23.3 This policy does not form part of the formal contract of employment, but is a condition of employment that employees will abide by. Any failures to follow the policy can therefore result in disciplinary proceedings. All staff are to sign the 'Staff Data Protection Agreement' attached at Appendix 4.

23.4 This Policy will be kept under review by the board of trustees. The last review was in October 2021.

24. APPENDICES

1. Privacy Notices (Pupils/Staff)
2. Subject Access Request (SAR) Form
3. Data Breach Reporting Form
4. Staff Data Protection Agreement
5. Data Privacy Impact Assessment (DPIA)
6. School Records Retention Schedule.

APPENDIX 1

Mayville Primary School
PRIVACY NOTICE
(How we use pupil information)

Our commitment

The trustees of Mayville Primary School are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place, which complies with existing laws and abides by the data protection principles.

Mayville Primary School is categorised as a data controller and is registered with the Information Commissioner's Office (ICO) – Registration Number: ZA174601.

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)
- Medical, accident logs, home address and next of kin information for use with emergency services, statutory assessment services, doctors' surgeries, school nursing service and social care.
- Contact details (home address, email address and telephone numbers)
- Assessment information (such as attainment and progress records across curriculum subjects)
- Behavioural information (types of behaviour displayed, outcomes of incidents and number of exclusions)
- Safeguarding information (detail of disclosures, outcomes of meetings, various plans and sensitive information regarding court proceedings, child protection plans and correspondence with outside agencies.)
- Educational History (such as prior and previous schools)
- Financial information (such as online payments, dinner money, trip payments and voluntary contributions)
- Admissions information (such as Supplementary Admissions Form information, Looked After Child status, widow/widower status and church attendance information)

- Health & Safety information (such as records of minor injuries and information that is required to comply with the Health & Safety Executive (HSE) RIDDOR requirements.
- Static and moving images (such as photographs of pupils and CCTV recordings)
- Exclusions information (such as start date, number of days, category, reason and correspondence to parents)
- Special Educational Need information (such as provision, needs, placements, payments, medical information, care information)
- Medical information (such as medical need, GP contact data, specialist contact details)
- School history (such as school name, dates attended)
- Parent/Carer information (such as name, address, contact details)
- Emergency contact information (such as name, address, contact details)
- Biometric data.

Why we collect and use this information

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing;
- to comply with statutory request for data from relevant authorities.

The lawful basis on which we use this information

We process the personal data detailed above in accordance with Article 6 of the GDPR. Personal information will only be collected and used with your consent or where it is needed by the school or the local authority to comply with a legal obligation or to fulfil a public task. For example, the Education Act 1999 requires the collection of pupil data for school census purposes.

Special category data (for example ethnicity, health or biometric data) is processed in accordance with Article 9 of the GDPR. It will usually only be collected and used with your explicit consent or where there is substantial public interest in the processing which enables the school to comply with a legal obligation.

For further information on how data is used, please visit the following website
https://www.gov.uk/education/data-collection-and-censuses-for-schools

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 if you have a choice in this.

Storing pupil data

We hold pupil data for the length of time prescribed in the HCC 'Retention Schedule for Schools', which has been created to assist schools to manage their information in line with the current legislative framework.

Who we share pupil information with

We routinely share pupil information with:

- Educational establishments that the pupil's attend after leaving us
- The Local Authority
- The Department for Education (DfE)
- Social care and the NHS (such as the School Nursing Service)
- Statutory assessment services
- Our feeder schools
- Organisations which provide learning tools
- Organisations which provide registration tools (SIMS)
- Organisations which provide Information Management Services (SIMS)
- Organisations which provide data collection, monitoring and reporting services (such as software from DfE)
- Organisations which provide cloud storage solutions (such as Strictly Education)
- Organisations which provide ICT support services (such as Strictly Education)
- Organisations which support our Pastoral Care systems(CPOMS)
- Organisations which provide Virtual Learning Environments
- Organisations which provide communication services (PAY360)
- Other local authorities if they have responsibility for a child has SEN/LAC
- Daily attendance will be shared with the London Borough Of Waltham Forest commissioned service called Social Services for all 'Looked After Children' attending this school.

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.

We share pupils' data with the Department for Education (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 our local authority (LA) and the Department for Education (DfE) under section 3 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 Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

For more information about services for young people, please visit our local authority website: London Borough of Waltham Forest.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education 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 Department has robust processes in place to ensure the confidentiality of our 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 department'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. To make a request for your personal information, or be given access to your child's educational record, contact the school's business manager.

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
- 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.

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:

Lorraine Barella, Kerry Day or Rose De La Cuesta

Email: Lorraine.barella@mayville.waltham.sch.uk

If you need more information about how our local authority and/or DfE collect and use your information.

Or visit, the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

APPENDIX 1B

Mayville Primary School
PRIVACY NOTICE
(How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- Personal information (such as name, employee or teacher number, national insurance number).
- Special categories of data including characteristics information such as gender, age, ethnic group.
- Contract information (such as start dates, hours worked, post, roles and salary information).
- Work absence and attendance information (such as number of absences and reasons, also attendance on site).
- Qualifications (and, where relevant, subjects taught).
- Bank account information for payroll purposes.
- Medical, home address and next of kin information for use with emergency services.
- Contact details (home address, email address and telephone numbers).

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.
- Enable individuals to be paid.
- Enable individuals to be treated for medical purposes.
- Contact staff outside of school hours in an emergency.
- Report back to the Department for Education on statutory workforce census returns.

The lawful basis on which we process this information

We process this information under 'GDPR article 6' in respect of public task and from 'GDPR article 9' where data processed is categorised as special category data.

For further information on how data is used, please visit the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of your data 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.
It will usually only be collected and used with your explicit consent or where there is substantial public interest in the processing which enables the school to comply with a legal obligation.

Storing this information

We hold school workforce data for the length of time prescribed in the HCC 'Retention Schedule for Schools', which has been created to assist schools to manage their information in line with the current legislative framework.

Who we share this information with

We routinely share this information with:

- Our local authority.
- The Department for Education (DfE).
- Organisations which provide financial services (such as Strictly Education).
- Organisations which provide registration tools (SIMS).

Why we share school workforce information

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

Local Authority

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.

Department for Education (DfE)

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 school employees with our local authority (LA) and the Department for Education (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.
- 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. To make a request for your personal information, contact the school data protection officer.

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.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with the school's Data Protection Officer.

Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:

Lorraine Barella or Kerry Day

Data Protection Officer (DPO)

Mayville Primary School

Lincoln Street

London

E11 4PZ

Email: Lorraine.barella@mayville.waltham.sch.uk

APPENDIX 2

Mayville Primary School

SUBJECT ACCESS REQUEST FORM (SAR)

Name of submitting person: ……

Name of individual whose information is being requested:

……

Name of authorised authority: ……

Please provide two appropriate identification types at the time of submitting this form, in person. No personal information will be recorded from your proof of identification. We will not release an individual's personal information until we are satisfied who is raising the request is either the intended recipient or a member of a legitimate authorised organisation *(Police, Social Services, Solicitor).*

Accepted proofs of identification include: Current Passport, Current Driving License, Utility bill (less than 3 months old).

Please complete the boxes below

Information Detail Requested	**Date Requested**	**Date Issued**

Please note

Parents/guardians or authorities requesting information relating to children's personal data that we process and store on behalf of our students/staff will need to submit a Subject Access Request (SAR) form via the school's data protection officer.

We will seek advice in every case, from the Information Commissioner Office (ICO) prior to releasing requested information relating to children.

Adults submitting a SAR may be required to provide more information relating to a request. In these circumstances, we will respond to you within 40 calendar days of submitting this SAR form.

However, if any of the information requested is in the educational record, then the school will respond in 15 school days. The record is free to view, however a charge will be applied if copies are required.

Your request may be withheld due to a lawful exemption or where the information might cause serious harm to the physical or mental health of the pupil or another individual. If this is the case please see our reasons below:

If you are unhappy with the result or information released from this SAR, please contact the Information Commissioners Office to whom we recommend you seek advice on

Tel: 0303 123 1113.

APPENDIX 3

DATA BREACH INCIDENT REPORTING FORM

Send completed forms as soon as possible, to Data Protection Officer.
Provide as much information as you can, but do not delay sending in the form.

GENERAL DETAILS	
Name of person reporting:	
Department:	
Contact number:	
Date form completed:	
Date of incident:	
Location of incident	
ABOUT THE INCIDENT	
Incident description. What has happened?	
Was personal information lost or compromised?	
If yes, was <u>sensitive</u> personal data compromised? *This is data relating to health, social care, public health, ethnicity, sexual life, trade union membership, political or religious beliefs, criminal offences, genetic or biometric data.*	
What information does it relate to? E.g. a file containing pupils details, or staff addresses	
How many people does the information relate to?	
What medium was the information held on? - Paper, USB stick, Laptop, etc.	
Dealing with the incident: **Please list initial actions: -** Who has been	

informed? What has been done?	
Has any action been taken to prevent recurrence?	
Are further actions planned? If so, what?	

Incident management	
If electronic, was the data encrypted?	Yes/No
Have the staff involved in the security incident done any Data Protection Training?	Yes/No
Has the data subject been informed?	Yes/No
Has the line manager been informed?	Yes/No
IT Services informed (if the incident involves the loss or theft of IT Equipment)?	Yes/No

Who to contact for advice:

Lorraine Barella, Data Protection Officer (DPO)
Email: Lorraine.barella@mayville.waltham.sch.uk or Ext 141

APPENDIX 4

DATA PROTECTION AND CONFIDENTIALITY STATEMENT

Staff and Trustees

I confirm that I have read the Data Protection Policy and adhere to the clauses within them with regard to confidentiality and data protection.

For the purposes of this document, 'Personal Data' includes all personal and sensitive data for children and staff.

I undertake to follow the procedures below to ensure that personal data is secure:

- All personal data held must be accurate, relevant and secure.
- Explicit consent must be sought for collecting and sharing data for purposes other than for a legal basis, such as using photographs or completing surveys (Admin retain all student consent forms).
- Documents which hold personal data will be kept secure.
- If documents are removed from the school for an approved purpose, they will be carried safeguarded at all time (paper files) or on an encrypted data stick (electronic). The Headteacher's approval is required prior to the removal of personal data from the school.
- Passwords will be kept confidential, secure and changed as per network policy.
- Any loss or potential loss of data or breaches of confidentiality must be reported immediately to the Data Protection Officer (DPO).
- For the purposes of taking books home for marking, books must be kept securely during transportation (public transport must not be used). Children will be advised not to use photographs on their books.
- Passwords for the computer system and (SIMS) must not be on display or easily found on desks, if you write down passwords they must be kept locked away at all times.
- Computers must be locked or shut down when leaving the room.
- Online tools or systems that require the use of personal data (student/staff) are not to be used without consultation with the Headteacher.
- School personal data will not be held on personal computers at home.
- All staff will ensure that they possess no personal data on home computers, non-encrypted data sticks, hard drives or in paper form.
- Emails containing personal data will only be sent when there is no other option and only to other e-mail addresses known to be secure and accessed only by the intended recipient.
- Minutes of meetings should use initials and not full names.

Name: …… Signed: …… Date: ……

Examples of Data Breaches include, but are not limited to the following, and are potential disciplinary breaches:

- *Sending e-mails / letters to the wrong address.*
- *Leaving files containing confidential information in a public place.*
- *Staff removing information from school, which they are not permitted to.*
- *Failing to keep personal details of separated parents confidential.*
- *Sending confidential information by unsecured post which goes missing.*

APPENDIX 5

DATA PRIVACY IMPACT ASSESSMENTS (DPIA)

Guide to completing a DPIA

A DPIA is a process which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The General Data Protection Regulation (GDPR) will make it a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a **high** risk to the privacy of individuals.

Examples might include use of new technologies, including proposals to use cloud storage facilities for school information, use of software that uses details from the SIMS database, use of CCTV and biometrics, such as finger print scanning.

A DPIA can be used to help you to design more efficient and effective ways for handling personal data, minimise privacy risks to the individuals affected and financial and reputational impact of a data incident on the school.

This guide is intended to help you assess whether a DPIA is needed, identify levels of risk of personal data for your project and complete a DPIA report (where applicable), which will need to be agreed and approved by (complete as appropriate – Headteacher/Data Protection Officer).

When to carry out a DPIA

A DPIA should be completed when the project is likely to involve collection of personal data that may involve a high risk to the privacy of individuals. You should take into account the following when deciding whether a DPIA is necessary.

1. If personal data is not being collected or processed there is no need to do a DPIA.

2. Will the project involve the collection of new or different types of information about individuals? If personal information will be collected using new technology, or collection of a new type of special category data not collected before, you should carry out a DPIA. If you will be collecting large amounts of personal information to use in a way not previously used, you should complete a DPIA.

4. Any project involving monitoring of individuals, such as installation of new CCTV, should always require a DPIA as should any use of biometric technology.

When to start a DPIA

If you are thinking about starting a project or making changes to existing services/ systems, then you should consider whether a DPIA is necessary from an early stage.

A DPIA should be started at project initiation stage, continued throughout the life of the project and re-visited in each new project phase, for example, when you want to use the personal data for a new or additional purpose for the use of the data, or if you are collecting new personal data. This should be proportionate to the level of special category data being collected or processed as a result of the project.

It is important to start at an early stage of the process to allow for time to resolve issues and mitigate for any risks identified, in order to avoid the difficulties of having to address these points late in the project when other decisions have already been made.

How to carry out a DPIA

Use the checklist below to help you decide whether the project involves privacy risks, identify what they are and work out what steps you will need to take to minimise those risks as far as possible.

When you have considered all of the risks, you should come to a conclusion about anything you can do to eliminate or minimise the risks you have identified. Some examples might include:-

- Minimising the risks of collecting too much personal information on CCTV by siting and angling the cameras so that they are focussed only on perhaps the car park rather than the entire school playground, or the entrance door, not into the school office.
- Checking the questions you have asked on a form before you send it out and ensuring that you really need all of the personal information you have requested
- If you need to store personal information on paper records ensuring that you keep them in a secure location which cannot be readily accessed by unauthorised individuals.
- If using a laptop in a classroom, make sure that staff are instructed to lock the screen if they leave it unattended for a while.

When you have recorded all of these points and how you will address the risks, you should get it signed off – either by the Data Protection Officer (or if the Data Protection Officer is completing the form, by the Headteacher) and keep a copy to refer back to for audit purposes and for updating if the project is changed or extended in future.

Completing a DPIA

When you have completed the DPIA, considered any risks and mitigated them wherever possible, the school will need to decide whether to accept any remaining risks. It is good practice to document what risks were identified, what steps were taken to minimise them and what risks were accepted.

You will also need to consider who should sign off the final DPIA – e.g. Headteacher, Data Protection Officer.

You can find more detailed guidance on conducting privacy impact assessments on the ICO's DPIA code of practice

https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

DPIA Checklist

Project name: ……..

Brief description of project: ……..

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. students, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g. information about an individuals physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.

4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?
5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.

7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature: …….. Name (printed): ……. Position: …… (Headteacher or DPO) Date: ……..

APPENDIX 6

School Records Retention Schedule

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
1.0	School Governors					
1.1	Instruments of government, including Articles of Association	No		Permanent	**Permanent** Retain in school while current; when no longer required	
1.2	Records for all full trustees body, committee and panel meetings, including: a) agendas b) any report, statutory policy	Yes*	School Governance (England) Regulations (2013)	Permanent	**Permanent, or as below** Single copy of signed minutes, agenda and papers: retain in school for 6 years from date of meeting then	***If meeting deals with confidential staff issues**

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
	(including Admissions Policy) or other paper considered at governing body meeting c) signed minutes				Inspection copies: retain in school for current year + 3 then destroy as confidential waste or delete securely Additional copies: destroy as confidential waste or delete securely from electronic systems	
1.3	Trustees application forms - successful candidates	Yes		End of term of office + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.4	Trustees application forms - unsuccessful candidates	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.5	Trustees election voting forms	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
1.6	Trustees - registers and declarations of pecuniary interests	Yes		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.8	Action plans created and / or administered by the board of Trustees	No		Life of action plan + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	
1.9	Records relating to complaints dealt with by the board of trustees	Yes		Date of resolution of complaint + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	**It may be appropriate to review for further retention in the case of contentious disputes**
1.10	Annual parents' meetings			Permanent	**Permanent, or as below** Retain in school for 6 years from date of meeting then: Minutes and reports: All other records: destroy as confidential waste or delete securely from	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
					electronic systems*	
2.0	**Management and Administration**					
2.1	Log books of activity in the school, maintained by teachers	Yes[1]		Permanent	**Permanent** Retain in school whilst operationally required	
2.2	Head teacher's official diary	Yes[1]		Current academic year + 3 years	**Destroy** Delete securely or destroy as confidential waste*	Unless used as retrospective record of events

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.3	Minutes of the senior management team and other internal administrative bodies	Yes[1]		Permanent	**Permanent, or as below** Retain in school for 5 years from date of meeting then: Minutes dealing with strategic or policy matters: All other records: destroy as confidential waste or delete securely from electronic systems	
2.4	Reports made by the head teacher or the management team	Yes[1]		Retain in school for date of report + 3 years	**Permanent**	
2.5	Correspondence and general filing created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	
2.6	Professional development plans	Yes		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.7	School development plans	No		Retain in school for closure of file + 6 years	**archive**	
2.8	Employers' liability certificate	No		Permanent while school is operational	**Destroy** Destroy as confidential waste or delete securely from electronic systems once school closes	
2.9	School brochure/prospectus	No		Retain in school for current academic year + 3 years	**archive**	
2.10	Circulars to staff and pupils	No		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.11	Newsletters to parents	No		Retain in school for current academic year + 3 years	**archive**	
2.12	Visitors' books and signing in sheets	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.13	PTA (Parent Teacher Association) / old pupils' associations records	Yes		Retain in school for current academic year + 6 years	**archive or as below** Minutes, newsletters and membership registers: All other records: destroy as confidential waste or delete securely from electronic systems	
3.0	**LA (Local Authority)**					
3.1	Secondary transfer sheets (primary)	Yes		Current academic year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
3.2	Attendance returns	Yes		Current academic year + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
3.3	Circulars from the LA	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.0	**DfE (Department for Education)**					
4.1	School census returns	Yes	Education (School Performance Information) (England) Regulations 2007	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.2	OFSTED reports	No		Retain in school while current; replace former report with any new inspection report	**Permanent** *	*Reports should be available on the OFSTED website. Retain at least two previous reports if not available online.
4.3	OFSTED-related papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
4.4	Returns to the DfE	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.5	Circulars from the DfE	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.0	**Pupils**					
5.1	Records relating to the creation and implementation of the school's Admissions Policy	No	School Admissions Code (2014)	Retain in school for life of the policy + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.2	Admission forms: unsuccessful or withdrawn applications (including supplementary information e.g. proof of address, religion, medical conditions etc.)	Yes	School Admissions Code (2014)	a) If no appeal, 1 year from receipt b) If appealed, 1 year from resolution of case*	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*Records relating to appeals retained by Appeals Panel for 22 years from date of birth of pupil

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.3	Admission forms: successful applications	Yes	School Admissions Code (2014)	Date of admission + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Ensure that supplementary information e.g. proof of address, religion, medical conditions is added to the pupil's file
5.4	Admission registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Retain in school until date of last entry in the book (or file) + 3 years	**Permanent**	**If held electronically, a printout should be made at least** annually**. Any corrections made to electronic data should be clearly shown in the printout.**
5.5	Attendance registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Date of register + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.6	Pupil absence letters / leave forms / correspondence relating to authorised absence	Yes		Date of absence + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.7	Absence books	Yes		Current year + 6 years from last entry in book	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.8	Telephone message books for recording absences (sickness) or changes to pick up arrangements, etc.	Yes		Current year + 6 years from last entry in book	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.9	Child protection files • **Primary**	Yes	DfE 'Keeping Children Safe in Education' (2016), Annex B, p.61	Retain while the pupil remains at the primary school*	Follow guidelines in 5.13 for pupils transferring to another school	*CP information must be kept separate from the main pupil file. Where children leave the school or college ensure their child protection file is transferred to the new school or college as soon as possible. This should be transferred separately from the main pupil file, ensuring secure transit. Confirmation of receipt should be obtained
5.11	Pupil's educational record (pupil file) **Pupils with Special Educational Needs (SEN)** • **Primary**	Yes	Retain while pupil remains at the primary school	Retain while the pupil remains at the primary school*	Follow guidelines in 5.13 for pupils transferring to another school	Includes: • SEN reviews • Individual Education Plans (IEPs) / pupil profiles • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.13	Pupil's educational record (pupil file) **All other pupils** • **Primary**	Yes	The Education (Pupil Information) (England) Regulations 2005	Retain while the pupil remains at the primary school, then: a) Pupil transfers to a known Local Authority primary or secondary school in Hampshire b) Pupil transfers to a known Local Authority or independent primary / secondary school which is another county within the UK; or transfers to an independent school within Hampshire/ Portsmouth c) Pupil transfers to a known primary / secondary school outside of the UK	**The file should follow the pupil when he/she leaves primary school:** a) Send pupil record to new school[2] b) Send pupil record to new school, retaining a copy or summary until pupil is 22 years old, then destroy confidentially or delete securely c) Send a copy of pupil record to new school, retaining original pupil record until pupil is 22 years old, then destroy confidentially or delete securely	Includes: • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered

[2] In the case of exclusion it may be appropriate to transfer the record to the Education and Inclusion Service

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
				d) Pupil transfers to an unknown school	d) Retain pupil file until pupil is 22 years old, then destroy confidentially or delete securely	
5.15	Pupil's educational record (pupil file) • Deceased pupils	Yes		Date of death + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.16	Images of pupils - signed consent forms by parent / guardian	Yes		Date of signing + 5 years; or at end of project; or when pupil leaves the school	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Images should not be reused outside of the time period or for other projects other than that specified on the form
5.17	Activity / visit / trip consent forms - signed by parent or guardian where no incident occurs	Yes		Date of event + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.18	Activity / visit / trip consent forms - signed by parent or guardian where a major incident occurs	Yes	Limitation Act 1980	Date of birth of child involved in incident + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	**Important:** consent forms for ALL pupils for an event where a major incident occurs must be retained, not just that of the child involved
5.19	Punishment books	Yes		Books no longer maintained in schools	**Permanent**	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.20	SATS papers (completed)	Yes	Department for Education (DfE) recommendation	Current year + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.21	SATS results for individual pupils	Yes			Add to the main pupil file and follow retention period for 5.14	
5.22	Internal and external examination papers (completed)	Yes		Current academic year + 6 years or until any appeals / validation process is complete	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.23	Internal and external examination results for individual pupils	Yes			Add to the main pupil file and follow retention period for 5.14*	*Uncollected GCSE and A Level certificates should be returned to the relevant examination board
5.24	Examination results - summaries or other statistical information created by the school	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.26	Any other records created in the course of contact with pupils maintained for teachers' own use (i.e. NOT part of the educational record)	Yes		Current academic year + 3 years	**Review** Review by school and EITHER allocate further retention period OR destroy as confidential waste or delete securely from electronic systems	
6.0	**Curriculum**					
6.1	Curricular records	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	May include: • curriculum development records • lesson plans • syllabuses • schemes of work • timetables • mark books • records of homework set

7.0	**Human Resources**					
7.1	Interview notes and recruitment records (including pre-employment vetting information) • unsuccessful candidates	Yes	PCC corporate guidelines	Date of interview + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Includes: • proof of identity • proof of right to work in the UK
7.2	Interview notes and recruitment records (including pre-employment vetting information) • successful candidates	Yes		Follow retention period for 7.4	All recruitment information to be added to staff personnel file, except DBS checks (for DBS see 7.3)	
7.3	Pre-employment vetting information • successful candidates' DBS checks*	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Maximum of date of check + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems by the designated member of staff	(Name of school) School does not retain copies of DBS certificates.
7.4	Staff files (main personnel file)	Yes	Limitation Act (1980)	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
7.5	Staff annual appraisal / assessment records	Yes		Current appraisal year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.6	Staff timesheets	Yes	Financial regulations	Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.7	Staff sickness records, excluding ill-health referrals (self-certification, doctor's certificates)	Yes		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.8	Staff sickness records • ill health referrals	Yes	Limitation Act (1980)		Add to main personnel file and follow retention period for 7.4	
7.9	Staff maternity and paternity pay records	Yes	Statutory Maternity Pay Regulations (1986) (as amended)	Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.10	Disciplinary proceedings* • warnings	Yes			Add to main personnel file and follow retention period for 7.4	*for child protection / safeguarding disciplinary proceedings, see 7.13

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
7.11	Disciplinary proceedings* • substantiated or unsubstantiated	Yes		a) outcome letter: end of employment + 7 years b) all other records: close of case + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*for child protection / safeguarding disciplinary proceedings, see 7.13
7.12	Disciplinary proceedings* • false or malicious	Yes		a) outcome letter: end of employment + 7 years b) all other records: shred at close of case	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*for child protection / safeguarding disciplinary proceedings, see 7.13
7.13	Disciplinary proceedings* • safeguarding / child protection related	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Until normal pension age, or for 10 years from date of allegation, whichever is longer	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*including where the allegation is unsubstantiated
7.14	Records of industrial tribunals, disciplinary panels, appeals	Yes	Limitation Act 1980 can apply		a) outcome letter: add to personnel file and follow retention period for 7.4 b) all other records: shred 7 years from end of process	
7.15	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.0	**Health and Safety (H&S)**					
8.1	Health and safety policies	No		Life of policy + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.2	Risk assessments: general	No	Limitation Act (1980)	Date of risk assessment + 7 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.3	Risk assessments: exposure to noise, vibration, lead, asbestos, chemicals and biohazards (including COSHH)	No	Control of Substances Hazardous to Health Regulations (2002), Regulation 11 Control of Asbestos at Work Regulations (2012), Regulation 19	Date of risk assessment + 40 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.4	Risk assessments: exposure to radiation	No	Ionising Radiation Regulations 1999 (SI 1999/3232)	Date of risk assessment + 50 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.5	Accident reporting: adults a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Current year + 3 (b) Current year + 3 (c) Current year + 3	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Since April 2016 accident reporting has been completed online and all copies are held electronically
8.6	Accident reporting: children a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Keep books until youngest child entered has reached age 22 (b) Date of birth of child + 22 years (c) Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Since April 2016 accident reporting has been completed online and all copies are held electronically
8.7	Violent incident reporting (VIR)	Yes	Limitation Act (1980)	Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.8	Physical intervention forms	Yes		Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.9	Fire precaution log books (e.g. records of drills and tests)	No	Limitation Act (1980)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.10	Accessibility plans	Yes	Equalities Act (2010)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.11	Health and safety training records	Yes		While current + 6 years, unless records apply for limited period (e.g. First Aid Certificates)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.12	Maintenance records for any work equipment, including ladders, trollies, PPE, PAT etc.	No		Current year + 10 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.13	Health and safety inspection records, including: • site inspections • playground inspections	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.0	**Finance**					
9.1	Annual accounts	No		Retain in school for current year + 6 years	**archive**	
9.2	Annual budget and background papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.3	Budget reports and budget monitoring records	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.4	Records covered by various financial regulations Including: invoices, receipts, order books, requisitions, delivery notices, petty cash records, records relating to the collection and banking of monies, records relating to the identification and collection of debt	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.5	Copy orders	No		Current year + 2 years, or current year + 6 years if included with delivery notes, invoices and receipts, etc.	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.6	Loans and grants managed by the school	No	Financial regulations	Date of last payment on loan + 12 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.7	School Fund records Including: cheque books, paying-in books, ledgers, invoices, receipts, bank statements, journey books	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.8	Contracts: under seal		Limitation Act (1980)	Contract completion date + 13 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.9	Contracts: under signature		Limitation Act (1980)	Contract completion date + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.10	Contracts: monitoring records			Current year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.11	Free school meals records	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.12	School meals registers	Yes		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.13	School meals summary sheets	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	**Formerly known as M1 forms**

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.14	Applications for free school meals, travel, uniforms etc.	Yes	Financial regulations	Whilst child at school or current year + 6 years, whichever is the longest	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.15	Payroll records where school administers own payroll	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.16	Records relating to individuals' pension details	Yes	Financial regulations	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.0	**Property**					
10.1	Title deeds of all properties belonging to the school	No		Permanent	**Permanent** Retain in school whilst operational; when no longer required	
10.2	Plans of all properties belonging to the school	No		Permanent	**Permanent** Retain in school whilst operational; when no longer required	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
10.3	Leases of properties leased by or to the schools	No		Expiry of lease + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.4	Records relating to the letting of school premises	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.5	Burglary, theft and vandalism report forms			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.6	All records relating to the maintenance of the school, including maintenance log books	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.7	Inventories of equipment and furniture			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.8	Insurance papers			While current	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
11.0	**Adult and Community Learning and Activities**					
11.1	Annual funding agreements with Learning and Skills Council (LSC), Adult and Community Learning Unit, or colleges			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.2	Enrolment forms, fee receipts, refund records, course registers, banking records			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.3	LSC capital grants, expenditure records			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.4	Community management agreements			Life of agreement + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.5	Minutes of governors' management committees			Permanent	**Permanent** Retain in school for 6 years from date of meeting	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
11.6	Annual Community Service plans			While current + 6 years	**archive**	
11.7	Income records for centre-run activities			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.8	Notice of successful applications for external funding, and conditions attached to grants			Period of funding or length of funding agreement (e.g. capital schemes) + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.9	Adult learning course programmes and brochures			Current year + 3 years	**archive**	
11.10	Records relating to the letting of school facilities to community or other groups, including after-school and holiday clubs	Yes	Statute of Limitations 1980	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
12.0	**Miscellaneous**					
12.1	School magazines			While useful	**archive**	
12.2	Scrapbooks			While useful	**archive**	
12.3	Photo albums			While useful	**archive**	
12.4	School histories			While useful	**archive**	
12.5	Audio and video recordings			While useful	**archive**	