



# **WIMBLEDON PRIMARY FEDERATION**

## **DATA PROTECTION POLICY**

Approved: Chair of Governors

Headteachers

Date: 11 Jan 2023

Date 11 Jan 2023

Next revision: Jan 2024

## Introduction

Wimbledon Primary Federation (WPF) is committed to being transparent about how it collects and uses data in order to meet its data protection obligations. This policy sets out our commitment to the protection of data.

We may, from time to time, be required to share personal information about employees, pupils, students or trainees with other organisations, this includes Local Authorities, Department for Education, other schools and educational bodies, and potentially social services and law enforcement agencies.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how we comply with the principles of the GDPR.

Organisational methods for keeping data secure are imperative, and we believe that it is good practice to keep clear practical policies and written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. We have signed up to Merton's Data Protection Officer Service Level Agreement. The role of the DPO is to inform and advise us on our data protection obligations. The DPO can be contacted at [schoolsDPO@merton.gov.uk](mailto:schoolsDPO@merton.gov.uk)

## Legal framework

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

- The General Data Protection Regulation (GDPR) 2018
- 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
- The Data Protection Bill 2017-19 which will adopt the GDPR, DPLED and The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data into UK law in the wake of the UK's exit from the European Union.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner' Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Department For Education (2018) 'Data Protection: A toolkit for schools'

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

- Online-safety Policy
- Freedom of Information Policy

## Applicable data

Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')".

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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.

Sensitive personal data is referred to in the GDPR as '**special categories of personal data**'. These specifically include the processing of race; ethnic origin; politics; religion; trade union membership; genetics; biometrics where used for ID purposes); health; sex life; or sexual orientation.

## **Principles**

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

## **Accountability**

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

We will also provide comprehensive, clear and transparent privacy policies.

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

Internal records of processing activities will include the following:

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

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

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

Data protection impact assessments will also be used, where appropriate.

### **Data protection officer (DPO)**

This school participates in the Merton Council DPO SLA which provides a shared DPO for Merton Schools. In addition, the Headteacher is designated as the Chief Privacy Officer (CPO) and supports the DPO.

The DPO assists the Data Controller to inform and advise the school and its employees about our obligations to comply with the GDPR and other data protection laws, monitor our compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

The individual appointed as DPO has professional experience and knowledge of data protection law, particularly in relation to maintained schools.

The DPO reports to the highest level of management.

The DPO operates independently and will not be dismissed or penalised for performing their task.

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

The DPO will work alongside safeguarding leads to ensure that pupil/student data is protected as required.

### **Lawful processing**

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

Under the GDPR, data will be lawfully processed under one of the following conditions (Article 6):

- a) Consent of the data subject
- b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- c) Processing is necessary for compliance with a legal obligation
- d) Processing is necessary to protect the vital interests of a data subject or another person
- e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

In order to lawfully process special category data, we will identify both a lawful basis under Article 6 above and a separate condition for processing special category data under Article 9 below.

- a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

- d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- e) processing relates to personal data which are manifestly made public by the data subject;
- f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## **Consent**

When we use consent as a legal basis for processing data, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

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

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

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

Consent can be withdrawn by a data subject at any time.

## **The Right to be informed**

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

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

- a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- b) the contact details of the data protection officer;
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d) the legitimate interests pursued by the controller or by a third party;
- e) the recipients or categories of recipients of the personal data, if any;
- f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation with reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

- g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- j) the right to lodge a complaint with a supervisory authority;
- k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- l) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

### **The right of access**

Individuals have the right to obtain confirmation that their data is being processed and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

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

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

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

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

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

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

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

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

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

### **The Right to Rectification**

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

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

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

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

Where no action is being taken in response to a request for rectification, we 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.

## **The right to Erasure**

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

Individuals have the right to erasure in the following circumstances:

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

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

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

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

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

## **The Right to Restrict Processing**

Individuals have the right to block or suppress our processing of personal data. In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

We will restrict the processing of personal data in the following circumstances:

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

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

## **The Right to Data Portability**

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

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

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

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a Contract

- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. We will provide the information free of charge.

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

We use School 2 School (S2S), provided by Department for Education, to securely transfer pupil records to and from other schools in a machine readable format.

S2S is a secure data transfer website available to schools and Local Authorities in England and Wales.

S2S has been developed to enable all data files required by DfE or by Local Authorities on behalf of DfE or which schools need to send to each other to be sent securely.

WPF is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

We will respond to any requests for portability within one month.

### **The Right to Object**

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

Individuals have the right to object to the following:

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

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

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

Where personal data is processed for direct marketing purposes:

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

Where personal data is processed for research purposes:

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

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

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

Where no action is being taken in response to a request, we 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.



## Privacy by design and privacy impact assessments

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

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

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to this school'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.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- We will ensure that all DPIAs include the following information:
  - A description of the processing operations and the purposes
  - An assessment of the necessity and proportionality of the processing in relation to the purpose
  - An outline of the risks to individuals
  - The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

## Data Breaches

The GDPR identifies personal data breaches as follows:

- **"Confidentiality breach"** - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **"Availability breach"** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- **"Integrity breach"** - where there is an unauthorised or accidental alteration of personal data.

The Senior Leadership Team 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.

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 us becoming aware of it.

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

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

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

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

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

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

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

Failure to report a breach when required to do so may result in action by the Information Commissioner.

## **Data Security**

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

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

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. This school uses the LGFL Gridstore System for off-site backup.

Where data is saved on removable storage or a portable device, this device will be encrypted using Advanced Encryption Standard (AES) 256-Bit Security to FIPS-197 standard. Such devices will be kept in a locked filing cabinet, drawer or safe when not in use.

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

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

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

Staff and governors will not use their personal laptops, computers or other devices for school business unless they notify the school first. Any documents containing personal or confidential information should be stored and accessed under school systems. Local copies should be securely deleted after use.

Staff and governors will not use personal email accounts or personal cloud storage for school business.

Members of staff who access the school network are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Remote access to school systems is permitted based on a credible business case. When permission is granted remote access will be via LGFL CISCO anywhere client. Use of second factor authentication is mandatory for remote access to the school network. This includes the use of both 'soft' and 'hard' One Time Passwords.

Wi-Fi access to the school network is permitted from school devices. Staff owned devices and visitors must use the separate Guest Wi-Fi.

Access to files on the school network is on a need to know basis - files and folders have granular permissions based on staff seniority and role. File access is monitored and reviewed.

Email is not a secure medium for external communication and should be used as a last resort for sending sensitive or confidential information. If documents are sent by email they should be encrypted with a password.

This school uses the Secure Document Transfer Portal (USO-FX) provided by the LGFL to transfer information securely.

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

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

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices

under lock and key. The person taking the information from school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

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

Visitors to areas containing sensitive information are supervised at all times.

The physical security of our buildings and storage systems, and access to them, is reviewed regularly. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

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

The Data Protection Officer will assist in making sure that continuity and recovery measures are in place to ensure the security of protected data.

### **Publication of Information**

This school publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

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

This school will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

### **CCTV and photography**

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

We notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

We will always indicate our intentions for taking photographs of pupils and will retrieve permission before publishing them.

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

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

### **Data retention**

Data will not be kept for longer than is necessary. We document all information we hold and dispose of data according to our retention schedule.

The Department for Education recognise that further guidance is required in this area and we will incorporate any new standard approach into our record management practice as it emerges. <sup>1</sup>

Unrequired data will be deleted as soon as practicable.

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

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

A certificate of destruction will be obtained when computer hard drives that have held personal information are disposed of.

### **DBS data**

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

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

## Appendix 1 – Data Retention Schedule

### 1) Child Protection Files

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
1.1	Child protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	Date of birth + 25 years	Secure disposal
1.2	Allegation of child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance). Education Act 2002 Guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Secure disposal

## 2) Governors

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
2.1	Minutes	No		Permanent	Must be available in school for 6 years from the meeting. Can then be archived/stored elsewhere.
2.2	Agendas	No		Date of meeting	Secure disposal
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from report date. Can consider archiving/storing anything important.
2.4	Annual parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from meeting date. Can consider archiving/storing anything important.
2.5	Instruments of Government	No		Permanent	Retain in school whilst school open. Can then be archived/stored elsewhere.
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required. Can then be archived/stored elsewhere.
2.7	Action plans	No		Date of action plan + 3 years	Secure disposal
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy operational (this includes if the expired policy is part of a past decision making process).
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Review for further retention in the case of contentious disputes. Secure disposal.
2.10	Annual reports required by Dept of Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI2002 No1171	Date of report + 10 years	Secure disposal
2.11	Proposals for schools to become or be established as Specialist Status schools	No		Current year + 3 years	Secure disposal

### 3) Management

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
3.1	Log books	Yes		Date of last entry in book + 6 years	Secure disposal
3.2	Minutes of the senior management team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in school for 5 years from meeting date. Can consider archiving/storing anything important.
3.3	Reports made by the head teacher or management team	Yes		Date of report + 3 years	Retain in school for 3 years from report date. Can consider archiving/storing anything important.
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	Secure disposal
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No/Yes		Date of correspondence + 3 years	Secure disposal
3.6	Professional development plans	Yes		Closure + 6 years	Secure disposal
3.7	School development plans	No		Closure + 6 years	Review for further retention. Secure disposal.
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	Secure disposal
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	Secure disposal
3.10	Admissions - secondary schools - casual	Yes		Current year + 1 year	Secure disposal
3.11	Proof of address supplied by parents as part of the admissions process	Yes		As the corresponding admission record	Secure disposal
3.12	Supplementary information form including additional information such as religion, medical conditions supplied as part of the admissions process	Yes		As the corresponding admission record	Secure disposal

#### 4) Pupils

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
4.1	Admission registers	Yes		Entry + 7 years	Retain in school for 7 years from entry. Can consider archiving these records if have the facility.
4.2	Attendance registers	Yes		Date of register + 3 years	Secure disposal
4.3	Pupil files retained in schools	Yes		Retain for time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.4	Pupil files	Yes		Retain for time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.5	Special Educational Needs files, reviews and individual education plans	Yes		Date of birth + 25 years	Secure disposal
4.6	Correspondence relating to authorised absence and issues	Yes		Date of absence + 2 years	Secure disposal
4.7a	Public Examinations	No		Year of examination + 6 years	Secure disposal
4.7b	Internal examination results	Yes		Current year + 5 years	Secure disposal
4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and retain with pupil file if necessary. Secure disposal
4.9	Statement maintained under the Education Act 1996 Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	Secure disposal unless legal action is pending



	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
4.12	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	Secure disposal unless legal action is pending
4.13	Parental permission slips for school trips, where there has been no major incident	Yes		Conclusion of the trip	Secure disposal unless legal action is pending
4.14	Parental permission slips for school trips, where there has been a major incident	Yes	Limitation Act 1980	Date of birth of pupil involved in the incident + 25 years	Secure disposal. Permission slips for all pupils on trip need to be retained for period to show that the rules had been followed for all pupils.
4.15	Records created by schools to obtain approval to run an educational visit outside the classroom, primary schools	No	3 part supplement of the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 14 years	Secure disposal
4.16	Records created by schools to obtain approval to run an educational visit outside the classroom, secondary schools	No	3 part supplement of the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 10 years	Secure disposal
4.17	Walking bus registers	Yes		Date of register + 3 years	This takes into account that if an incident requiring an accident report, the register will be submitted with the accident report and kept for the retention time for accident reporting. Secure disposal

## 5) Curriculum

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
5.1	School development plan	No		Current year + 6 years	Secure disposal
5.2	Curriculum returns	No		Current year + 3 years	Secure disposal
5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.5	Class record books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.6	Mark books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.8	Pupils' work	Yes		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.9	Examination results	Yes		Current year + 6 years	Secure disposal
5.10	SATs records, examination papers and results	Yes		Current year + 6 years	Secure disposal
5.11	PAN reports	Yes		Current year + 6 years	Secure disposal
5.12	Value added and contextual data	Yes		Current year + 6 years	Secure disposal
5.13	Self evaluation forms	Yes		Current year + 6 years	Secure disposal

## 6) Personnel Records held in Schools

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	Secure disposal
6.2	Staff personnel files	Yes		Termination + 25 years	Secure disposal
6.3	Interview notes and recruitment records	Yes		Date of interview notes + 6 months if unsuccessful. If successful place in personnel file.	Secure disposal
6.4	Pre-employment vetting information (including CRB checks)	Yes	CRB guidelines	Date of check + 6 months	Secure disposal
6.5	Disciplinary proceedings	Yes	Where the warning relates to child protection issues see 1.2		
6.5a	<i>Oral warning</i>	Yes		Date of warning + 6 months	Secure disposal
6.5b	<i>Written warning - level one</i>	Yes		Date of warning + 6 months	Secure disposal
6.5c	<i>Written warning - level one</i>	Yes		Date of warning + 12 months	Secure disposal
6.5d	<i>Final warning</i>	Yes		Date of warning + 18 months	Secure disposal
6.5e	<i>Case not found</i>	Yes		If child protection see 1.2, otherwise destroy immediately	Secure disposal
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years	In case of serious accidents a further retention period will need to be applied. Secure disposal
6.7	Annual appraisal and assessment records	Yes		Current year + 5 years	Secure disposal
6.8	Salary cards	Yes		Last date of employment + 85 years	Secure disposal
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	Secure disposal

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	Secure disposal
6.11	Proofs of identity collected as part of the process for checking "portable" enhanced CRB disclosure	Yes		Where possible these should be checked and a note/copy of what was checked placed on personnel file. If felt necessary to keep any documentation this should also be placed in personnel file.	Secure disposal of notes/copies and return of originals.

## 7) Health and Safety

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
7.1	Accessibility plans	Yes	Disability Discrimination Act	Current year + 6 years	Secure disposal
7.2	Accident reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		Secure disposal
7.2a	Adults	Yes		Date of incident + 7 years	Secure disposal
7.2b	Children	Yes		Date of birth of child + 7 years	Secure disposal
7.3	COSHH			Current year + 10 years	Where appropriate an additional retention period may be allocated. Secure disposal
7.4	Incident reports	Yes		Current year + 20 years	Secure disposal
7.5	Policy statements			Date of expiry + 1 year	Secure disposal
7.6	Risk assessments			Current year + 3 years	Secure disposal
7.7	Process of monitoring areas where employees and persons are likely to have come in contact with asbestos			Last action + 40 years	Secure disposal
7.8	Process of monitoring areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	Secure disposal
7.9	Fire precautions log book			Current year + 6 years	Secure disposal

## 8) Administrative

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
8.1	Employer's liability certificate			Closure of school + 40 years	Secure disposal
8.2	Inventories of equipment and furniture			Current year + 6 years	Secure disposal
8.3	General file series			Current year + 5 years	Review to see if further retention period required. Secure disposal
8.4	School brochure or prospectus			Current year + 3 years	Disposal
8.5	Circulars (staff, parents, pupils)			Current year + 1 year	Review to see if further retention period required. Secure disposal
8.6	Newsletters, ephemera			Current year + 1 year	Review to see if further retention period required. Secure disposal
8.7	Visitors book			Current year + 2 year	Review to see if further retention period required. Secure disposal
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see if further retention period required. Secure disposal

## 9) Finance

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
9.1	Annual accounts		Financial Regulations	Current year + 6 years	Secure disposal
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Secure disposal
9.3	Contracts				
9.3a	<i>Under seal</i>			Contract completion date + 12 years	Secure disposal
9.3b	<i>Under signature</i>			Contract completion date + 6 years	Secure disposal
9.3c	<i>Monitoring records</i>			Current year + 2 years	Secure disposal
9.4	Copy orders			Current year + 2 years	Secure disposal
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	Secure disposal
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	Secure disposal
9.7	Annual budget and background papers			Current year + 6 years	Secure disposal
9.8	Order books and requisitions			Current year + 6 years	Secure disposal
9.9	Delivery documentation			Current year + 6 years	Secure disposal
9.10	Debtors' records		Limitations Act	Current year + 6 years	Secure disposal
9.11	School fund - Cheque books			Current year + 3 years	Secure disposal
9.12	School fund - Paying in books			Current year + 6 years	Secure disposal
9.13	School fund - Ledger			Current year + 6 years	Secure disposal
9.14	School fund - Invoices			Current year + 6 years	Secure disposal
9.15	School fund - Receipts			Current year + 6 years	Secure disposal
9.16	School fund - Bank statements			Current year + 6 years	Secure disposal
9.17	School fund - School journey books			Current year + 6 years	Secure disposal
9.18	Student grant applications	Yes		Current year + 3 years	Secure disposal
9.19	Free school meals registers	Yes		Current year + 6 years	Secure disposal
9.20	Petty cash books			Current year + 6 years	Secure disposal

## 10) Property

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
10.1	Title deeds			Permanent	These should follow the property
10.2	Plans			Permanent	Retain in school whilst operational. Can then be archived/stored elsewhere.
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	Secure disposal
10.4	Leases			Expiry of lease + 6 years	Secure disposal
10.5	Lettings			Current year + 3 years	Secure disposal
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	Secure disposal
10.7	Maintenance log books			Last entry + 10 years	Secure disposal
10.8	Contractors' reports			Current year + 6 years	Secure disposal



## 11) Local Authority

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
11.1	Secondary transfer sheets (primary)	Yes		Current year + 2 years	Secure disposal
11.2	Attendance returns	Yes		Current year + 1 year	Secure disposal
11.3	Circulars from LEA	Yes		Whilst required operationally	Review to see if further retention period required. Disposal

## 12) Department for Education

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
12.1	HMI reports			These do not need to be kept any longer	Secure disposal
12.2	OFSTED reports and papers			Replace former report with new inspection report	Review to see if further retention period required. Secure disposal
12.3	Returns			Current year + 6 years	Secure disposal
12.4	Circulars from Department of Education			Whilst required operationally	Review to see if further retention period required. Disposal

## 14) School Meals

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
14.1	Dinner register			Current year + 3 years	Secure disposal
14.2	School meals summary sheets			Current year + 3 years	Secure disposal

## 15) Family Liaison Officers and Home School Liaison Assistants

	<b>Basic File Description</b>	<b>Data Protection Issue</b>	<b>Statutory Provisions</b>	<b>Retention Period</b>	<b>Action at End of Administrative Life of Record</b>
15.1	Day books	Yes		Current year + 2 years	Review to see if further retention period required. Secure disposal
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school	Secure disposal
15.3	Referral forms	Yes		While the referral is current	Secure disposal
15.4	Contact data sheets	Yes		Current year then review	If contact is no longer active secure disposal
15.5	Contact database entries	Yes		Current year then review	If contact is no longer active secure delete
15.6	Group registers	Yes		Current year + 2 years	Secure disposal