



# SPELLBROOK C of E PRIMARY SCHOOL (VC)

Learn together- Enjoy together -Succeed together

*"In everything - in every circumstance - do to others as you would have them do to you."*

Matthew 7:12

## General Data Protection Regulations (GDPR) & Data Protection Policy

Policy includes:

APPENDIX A – Statutory & Non-Statutory Document Retention

<b>Document Information</b>			
<b>Policy Number:</b>	v3	<b>Section:</b>	GDPR
<b>Review Cycle:</b>	Annual	<b>Type:</b>	Statutory
<b>Reviewed by:</b>	FGB	<b>Ratified by FGB:</b>	10 November 2022
<b>Responsibility:</b>	Resources Committee	<b>Next Review:</b>	November 2023

The following amendments have been made to this policy since the 'ratified by' date.

Date	Page number	Section	Details of change

These changes / recommendations will be reviewed / ratified by Full Governing Body for the 'review cycle' as quoted above.

<b>Contents:</b>	<b>Page</b>
Statement of Intent	2
1. Legal Framework	3
2. Applicable Data	3
3. Principles	3-4
4. Accountability	4-5
5. Data protection officer (DPO)	5
6. Lawful processing	5-6
7. Consent	6
8. The right to be informed	7-8
9. The right of access	8
10. The right to rectification	8-9
11. The right to erasure	9
12. The right to restrict processing	10
13. The right to portability	10-11
14. The right to object	11
15. Automated decision making and profiling	12
16. Privacy by design and privacy impact assessment	12-13
17. Data breaches	13-14
18. Data security	14-15
19. Publication of information	15
20. Data retention	16
21. DBS data	16
<b>APPENDIX A - Statutory &amp; Non-Statutory Document Retention</b>	

## **Statement of intent**

Spellbrook C of E Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR.

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

This policy is in place to ensure all staff and governors 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 Spellbrook C of E Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

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

## 1. Legal framework

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

- The General Data Protection Regulation
- 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

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

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

- Guide to the Use of Social Media Images
- E Safety & Data Security Policy
- Freedom of Information & Publication Scheme

## 2. Applicable data

2.1. 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, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

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

## 3. Principles

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  - Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
  - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
  - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 3.2. The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

## **4. Accountability**

- 4.1. Spellbrook C of E 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.
- 4.2. The school will provide comprehensive, clear and transparent privacy policies.
- 4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:
- Are not occasional.
  - Could result in a risk to the rights and freedoms of individuals.
  - Involve the processing of special categories of data or criminal conviction and offence data.
- 4.4. Internal records of processing activities will include the following:
- Name and details of the organisation
  - Purpose(s) of the processing
  - Description of the categories of individuals and personal data
  - Retention schedules
  - Categories of recipients of personal data
  - Description of technical and organisational security measures
  - Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

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

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

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

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

5.1. A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- 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.

5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the school, which is the headteacher.

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

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

## **6. Lawful processing**

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

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

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3. Sensitive data will only be processed under the following conditions:

- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

## 7. Consent

- 7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- 7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 7.3. Where consent is given, a record will be kept documenting how and when consent was given.
- 7.4. 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.

- 7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- 7.6. Consent can be withdrawn by the individual at any time.
- 7.7. Where a child is under the age of 16 or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

## **8. The right to be informed**

- 8.1. 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.
- 8.2. 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.
- 8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:
- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
  - The purpose of, and the legal basis for, processing the data.
  - The legitimate interests of the controller or third party.
  - Any recipient or categories of recipients of the personal data.
  - Details of transfers to third countries and the safeguards in place.
  - The retention period of criteria used to determine the retention period.
  - The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
  - The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- 8.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- 8.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- 8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:



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

## **9. The right of access**

- 9.1. Individuals have the right to obtain confirmation that their data is being processed.
- 9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- 9.3. The school will verify the identity of the person making the request before any information is supplied.
- 9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- 9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- 9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 9.7. All fees will be based on the administrative cost of providing the information.
- 9.8. All requests will be responded to without delay and at the latest, within one month of receipt.
- 9.9. 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.
- 9.10. 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.
- 9.11. 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.

## **10. The right to rectification**

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

- 10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 10.5. 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.

## **11. The right to erasure**

- 11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 11.2. 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
- 11.3. 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
- 11.4. 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.
- 11.5. 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.

- 11.6. 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.

## **12. The right to restrict processing**

- 12.1. Individuals have the right to block or suppress the school's processing of personal data.
- 12.2. In the event that processing is restricted, the school 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.
- 12.3. The school will restrict the processing of personal data in the following circumstances:
- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
  - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
  - Where processing is unlawful and the individual opposes erasure and requests restriction instead
  - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
- 12.4. 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.
- 12.5. The school will inform individuals when a restriction on processing has been lifted.

## **13. The right to data portability**

- 13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 13.2. 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.
- 13.3. 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
- 13.4. Personal data will be provided in a structured, commonly used and machine-readable form.
  - 13.5. The school will provide the information free of charge.
  - 13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
  - 13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
  - 13.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.
  - 13.9. The school will respond to any requests for portability within one month.
  - 13.10. 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.
  - 13.11. 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.

## **14. The right to object**

- 14.1. 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.
- 14.2. 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.
- 14.3. Where personal data is processed for the performance of a legal task or legitimate interests:
  - An individual's grounds for objecting must relate to his or her particular situation.
  - The 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.
- 14.4. Where personal data is processed for direct marketing purposes:
  - The school will stop processing personal data for direct marketing purposes as soon as an objection is received.

- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

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

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

## **15. Automated decision making and profiling**

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

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

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

15.3. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

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

- The school has the explicit consent of the individual.

The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

## **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.

- 16.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.
- 16.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- 16.5. A DPIA will be used for more than one project, where necessary.
- 16.6. 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
- 16.7. The school will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
  - An assessment of the necessity and proportionality of the processing in relation to the purpose
  - An outline of the risks to individuals
  - The measures implemented in order to address risk
- 16.8. 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.

## **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.
- 17.2. The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- 17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- 17.5. 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.
- 17.6. 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.
- 17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- 17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

- 17.9. 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.
- 17.10. 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
- 17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

## **18. Data security**

- 18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- 18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 18.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- 18.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- 18.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- 18.6. All electronic devices are password-protected to protect the information on the device in case of theft.
- 18.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 18.8. Staff and governors will not use their personal laptops or computers for school purposes.
- 18.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 18.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 18.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

- 18.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- 18.13. 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.
- 18.14. 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.
- 18.15. 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.
- 18.16. 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.
- 18.17. Spellbrook C of E Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 18.18. The **SBM** is responsible for continuity and recovery measures are in place to ensure the security of protected data.
- 18.19. When disposing of data, paper documents will be shredded, and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.
- 18.20. The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:
- Whether data was shared
  - What data was shared
  - With whom data was shared
  - For what reason data was shared
  - Where a decision has been made not to seek consent from the data subject or their parent
  - The reason that consent has not been sought, where appropriate
- The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

## 19. Publication of information



- 19.1. Spellbrook C of E Primary School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
- Policies and procedures
  - Minutes of meetings
  - Annual reports
  - Financial information
- 19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.
- 19.3. Spellbrook C of E Primary School will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 19.4. 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.
- 19.5. 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.
- 19.6. Precautions, as outlined in the Guide to the Use of Social Media & Images are taken when publishing photographs of pupils, in print, video or on the school website.
- 19.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## **20. Data retention**

- 20.1. Data will not be kept for longer than is necessary.
- 20.2. Unrequired data will be deleted as soon as practicable.
- 20.3. 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.
- 20.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

## **21. DBS data**

- 21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 21.2. Data provided by the DBS will never be duplicated.
- 21.3. 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.

Policy Reference: GDPR-B-

GDPR & Data Protection Policy

Appendices sourced from: Information Management Toolkit for Schools - v5  
February 2016

## **Appendix A**

### **Statutory and Non-Statutory Retention Periods**

## **School Document Retention Management**

### **1. Management of the School**

- 1.1 Governing Body
- 1.2 Headteacher and Senior Management Team
- 1.3 Admissions Process

### **2. Human Resources**

- 2.1 Recruitment
- 2.2 Operational Staff Management
- 2.3 Management of Disciplinary and Grievance Processes
- 2.4 Health and Safety
- 2.5 Payroll and Pensions

### **3. Financial Management of the School**

- 3.1 Risk Management and Insurance
- 3.2 Asset Management
- 3.3 Accounts and Statements Including Budget Management
- 3.4 Contract Management
- 3.5 School Fund
- 3.6 School Meals Management

### **4. Property Management**

- 4.1 Property Management
- 4.2 Maintenance

### **5. Pupil Management**

- 5.1 Pupil's Educational Record
- 5.2 Attendance
- 5.3 Special Educational Needs

### **6. Curriculum Management**

- 6.1 Statistics and Management Information
- 6.2 Implementation of Curriculum

## **7. Extra Curricular Activities**

- 7.1 Educational Visits outside the Classroom
- 7.2 Walking Bus
- 7.3 Family Liaison Officers and Home School Liaison Assistants

## **8. Central Government and Local Authority**

- 8.1 Local Authority
- 8.2 Central Government

## 1. MANAGEMENT OF THE SCHOOL

1.1	Governing Body				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body Meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of.	SECURE DISPOSAL
1.1.2	Minutes of the Governing Body Meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			

	Principal set (signed)			PERMANENT	It the school is unable to store these then they should be offered to County Archives Service
	Inspection copies			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently.	SECURE DISPOSAL Or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents meeting held under section 33 of the Education Act 2002	No	Education Act 2002, section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.

1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan +3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy +3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	No		Date of the resolution of the complaint + minimum of 6 years then the review for a further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governors Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report +10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date of proposal accepted or declined +3 years	SECURE DISPOSAL

1.2	Headteacher and Senior Management Team				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the headteacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be a permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of the Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Headteacher or the management team	There may be data protection issues if the log book refers to individual pupils or		Date of the meeting + a minimum of 3 years then review	SECURE DISPOSAL



		members of staff			
1.2.4	Records created by headteachers deputy headteachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the log book refers to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by headteachers, deputy headteachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plan	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3	Admissions Process				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the School Admissions Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Department advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made	REVIEW Schools may wish to consider keeping the admission register permanently as soft enquires from past pupils to confirm the dates they attended the school

1.3.5	Admissions – Secondary Schools – Casual	Yes		School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014
1.3.7	Supplementary Information form including additional information such as religion, medical conditions	Yes			
	For successful admissions		This information should be added to the pupil file		SECURE DISPOSAL
	For unsuccessful admissions		Until appeals process completed		SECURE DISPOSAL

1.4	Operational Administration				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.4.1	General file series	No		Current year + 5 years the REVIEW	SECURE DISPOSAL
1.4.2		No		Current year + 3 years	STANDARD DISPOSAL
1.4.3		No		Current year + 1 year	
1.4.4		No		Current year + 1 year	

1.4.5		No		Current year + 6 years the REVIEW	SECURE DISPOSAL
1.4.6		No		Current year + 6 years the REVIEW	SECURE DISPOSAL

## 2. HUMAN RESOURCES

2.1 Recruitment					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidates + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidates	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS checks	No	DBS Update Service employers Guide June 2014: Keeping children safe in education. Statutory guidance	The school does not have to keep copies of the DBS certificates. If the schools does so, the copy must NOT be retained for 6 months	
2.1.5	Proofs of identity collected as part of the process of checking ‘portable’ enhanced DBS disclosure			Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be place on the member of staff’s personal file.	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	Yes	An employer’s guide to right to work checks (Home Office May 2015)	Where possible these documents should be added to the Staff Personal file (see below), but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than 2 years	

<b>2.2</b>	<b>Operational Staff Management</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Appraisal/Assessment records	Yes		Current year + 6 years	SECURE DISPOSAL

<b>2.3</b>	<b>Management of Disciplinary and Grievance Processes</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	Keeping children safe in education Statutory guidance for schools and colleges March 2015, Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned.	
2.3.2	Disciplinary	Yes			
	Oral warning			Date of warning + 6 months	SECURE DISPOSAL (If warnings are placed on personal files then they must be weeded from the file)
	Written warning – level 1			Date of warning + 6 months	
	Written warning – level 2			Date of warning + 12 months	
	Final warning			Date of warning + 18 months	
	Case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	

2.4	Health and Safety				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.4.1	Health & Safety Policy Statements	No		Life of the policy + 3 years	SECURE DISPOSAL
2.4.2	Health & Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury at work	Yes		Date of incident + 12 years in the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident reporting	Yes	Social Security (claims Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of accident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of substances Hazardous to Health (COSHH)	No	Control of substances Hazardous to Health Regulations 2002. SI 2002 No 2677. Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 no 632 regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of area where employees and persons are likely to have become in contact with radiation	No		Last action + 40 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5	Payroll and Pensions				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (S11986/1960) revised 1999 (S11999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995			Current year + 6 years	SECURE DISPOSAL



### 3. FINANCIAL MANAGEMENT OF THE SCHOOL

<b>3.1</b>	<b>Risk Management and Insurance</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

<b>3.2</b>	<b>Asset Management</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.2.1	Employer's Liability Insurance Certificate	No		Closure of the school + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Closure of the school + 6 years	SECURE DISPOSAL

<b>3.3</b>	<b>Accounts and Statements including Budget Management</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant Applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget Statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

<b>3.4</b>	<b>Contract Management</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current + 2 years	SECURE DISPOSAL

<b>3.5</b>	<b>School Fund</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.5.1	School Fund – Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

<b>3.6</b>	<b>School Meals Management</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Register	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	Yes		Current year + 3 years	SECURE DISPOSAL

#### 4. PROPERTY MANAGEMENT

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

4.2	<b>Maintenance</b>				
	<b>Basic File Description</b>	<b>Data Protection Issues</b>	<b>Statutory Provisions</b>	<b>Retention Period (Operational)</b>	<b>Action at the end of the administrative life of the record</b>
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current financial year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance of log books	No		Current financial year + 6 years	SECURE DISPOSAL

## 5. PUPIL MANAGEMENT

5.1	Pupil's Educational Record				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI2005 no 1437		
	Primary			Retain whilst the child remains at the primary school	<p>The file should follow the pupil when he/she leaves the primary school. This will include:</p> <ul style="list-style-type: none"> <li>To another primary school</li> <li>To a secondary school</li> <li>To a pupil referral unit</li> </ul> <p>If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period</p> <p>If the pupil transfers to an independent school, transfer to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space</p>

					to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the records from the Local Authority
	Secondary	Limitation Act 1980 (section 2)		Date of Birth of the pupil + 25	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board
	Internal			This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file	Yes	Keeping children safe in education Statutory guidance for schools and colleges March 2015. Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child Protection information held in separate files	Yes	Keeping children safe in education Statutory guidance for schools and colleges March 2015. Working together to safeguard children. A guide to inter-agency	DOB of the child + 25 years then review. This retention period was agreed in consultation with the Safeguarding children Group on the understanding that the principal copy of this	SECURE DISPOSAL – these records MUST be shredded

			working to safeguard and promote the welfare of children March 2015	information will be found on the Local Authority Social Services record	
--	--	--	---	---	--

5.2	Attendance				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Department advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3	Special Educational Needs				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 20)	Date of Birth of the pupil + 25 years	REVIEW NOTE: this retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a 'failure to provide a sufficient education' case. There is an element of business risk analysis involved in any decision to keep the records longer than the

					minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 section1	Date of Birth of the pupil +25 years. (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 section 2	Date of Birth of the pupil +25 years. (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 section 14	Date of Birth of the pupil +25 years. (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold

## 6. CURRICULUM MANAGEMENT

6.1	Statistics and Management Information				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination results (Schools copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records	Yes			
	Results	Yes			
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2	Implementation of Curriculum				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	Yes		Current year + 1 year	
6.2.2	Timetable	No		Current year + 1 year	
6.2.3				Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupil's Work	No		Where possible pupil's work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

## 7. EXTRA CURRICULAR ACTIVITIES



7.1	Educational Visits outside the Classroom				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers Panel National Guidance website <a href="http://oepng.info">http://oepng.info</a> specifically Section 3 – ‘Legal Framework and employer Systems’ and Section 4 – Good Practice	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom- Secondary Schools	No	Outdoor Education Advisers Panel National Guidance website <a href="http://oepng.info">http://oepng.info</a> specifically Section 3 – ‘Legal Framework and employer Systems’ and Section 4 – Good Practice	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips - where there has been no major incident	Yes	Limitation Act 1980 (section 2)	Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time
7.1.4	Parental permission slips for school trips - where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years. The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

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

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

## 8. CENTRAL GOVERNMENT AND LOCAL AUTHORITY

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

8.2	Central Government				
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information send from central government	No		Operational use	SECURE DISPOSAL