Extend Learning
Academies Network

# Data Protection Policy
## (Including GDPR and Retention)

| | | |
|---|---|---|
| Written by: | ELAN executive team | |
| Reviewed by: | ELAN Board | Date: 03/07/2018 |
| Ratified by: | Name: Iain Kilpatrick<br><br>Signed: Iain Kilpatrick<br><br>Chair of the Board | Date: 03/07/2018 |
| Adopted by Academies: | Bournville Primary School<br>Locking Primary School<br>Mead Vale Primary School<br>Mendip Green Primary School<br>Milton Park Primary School<br>Oldmixon Primary School<br>Walliscote Primary School<br>Windwhistle Primary School | |
| Review: | Annually | |
| Next Review Due By: | July 2019 | |

# Contents

Statement of Intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. The right to rectification
11. The right to erasure
12. The right to restrict processing
13. The right to data portability
14. The right to object
15. Automated decision making and profiling
16. Privacy by design and privacy impact assessments
17. Data breaches
18. Data security
19. Publication of information
20. CCTV and photography
21. Data retention
22. DBS data
23. Policy Review

## Statement of Intent

Extend Learning Academies Network (ELAN) and the schools that make up the multi academy trust (MAT) is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The MAT and/or its schools 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 ELAN complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and ELAN 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.

Signed by:

_____ CEO Date: _____

_____ Chair of Board Date: _____

## 1. Legal framework

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

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

1.2. This policy will also have regard for the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

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

- E-safety Policy
- Freedom of Information Policy
- Data Retention Schedule – Appendix A

## 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 and within our schools for FSM, SEN and Child Protection.

## 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. ELAN 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 MAT will provide comprehensive, clear and transparent privacy policies.

4.3. Additional internal records of the MAT’s processing activities will be maintained and kept up-to-date.

4.4. 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.

4.5. 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

4.6. The MAT 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.

4.7. 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 MAT and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the MAT'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 MAT, which is the Chief Executive Officer.

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 MAT in the performance of its tasks.)

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

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## 7. Consent

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 MAT 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, 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT will inform them of the rectification where possible.

10.3. Where appropriate, the MAT 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 MAT 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 MAT and its schools 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

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 MAT 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 MAT's processing of personal data.

12.2. In the event that processing is restricted, the MAT 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 MAT 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 MAT has verified the accuracy of the data
- Where an individual has objected to the processing and the MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT will consider whether providing the information would prejudice the rights of any other individual.

13.9. The MAT 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 MAT 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 MAT 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 MAT will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the MAT 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 MAT will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT 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 MAT will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the MAT 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 MAT's data protection obligations and meeting individuals' expectations of privacy.

16.3. DPIAs will allow the MAT to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the MAT'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
- The use of CCTV.

16.7. The MAT 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 MAT 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 Chief Executive Officer 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 MAT 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 MAT 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 MAT, 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 MAT 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 or MAT 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 MAT 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 schools or other MAT locations containing sensitive information are supervised at all times.

18.16. The physical security of the MAT's buildings and storage systems, and access to them, is reviewed regularly and formally on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

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

18.18. The Headteacher is responsible for continuity and recovery measures are in place to ensure the security of protected data. Appendix B details the appointed processor within each MAT location.

## 19. Publication of information

19.1. ELAN publishes information on its website that will be routinely made 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. ELAN will not publish any personal information, including photos, on its website without the permission of the affected individual, or a parent/guardian if the individual is a child.

19.4. When uploading information to the school and/or MAT websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

## 20. CCTV and photography

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

20.2. The MAT notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

20.4. All CCTV footage will be kept for a maximum of six months for security purposes; the Head of Operations is responsible for keeping the records secure and allowing access.

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

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

20.7. Precautions are taken when publishing photographs of pupils, in print, video or on the school/MAT website.

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

## 21. Data retention

21.1. Data will not be kept for longer than is necessary.

21.2. Unrequired data will be deleted as soon as practicable.

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

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

## 22. DBS data

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

22.2. Data provided by the DBS will never be duplicated.

22.3. 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.

## 23. Policy review

23.1. This policy is reviewed every two years by the CEO and the Headteachers.

The next scheduled review date for this policy is May 2020.

## 1. Child Protection

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Safeguarding Policies and procedures | No | Permanent | ARCHIVE | Transfer to archive for retention when new policy implemented. |
| Child Protection files | Yes | DOB + 25 years but review sensitive case files every 5-6 years thereafter | SHRED | Child protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university, for example). Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority.<br><br>Limitation periods can be dis-applied in criminal and civil abuse cases; to be weighed against rights under the GDPR and our insurers' requirements.<br><br>Special category data MUST be shredded and disposed of securely at the end of its administrative life |
| Allegations of a child protection nature against a member of staff | Yes | Until the person's normal retirement age, or 10 years from the date of the allegation if that's longer | SHRED | ICO Employment Practices Code: Supplementary Guidance 2.13.1 (Discipline, grievance and dismissal)<br><br>"Records of allegations about workers who have been investigated and found to be without substance should not normally be retained once an investigation has been completed. There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example, where the allegation relates to abuse and the worker is employed to work with children or other vulnerable individuals".<br><br>Summary record to be retained on confidential personnel file, and a copy given to the person concerned. |

## 1. Child Protection (continued)

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| DBS Disclosure Certificates | Yes | No longer than 6 months from decision on recruitment unless DBS specifically consulted | SHRED | Keep a record in the Single Central Record that checks were undertaken, with relevant reference details (Disclosure number, date, who checked it). . |

## 2. Governors

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Minutes – principle set (signed) | Yes | Permanent | ARCHIVE | Transfer to archive for permanent retention after 6 years |
| Minutes – inspection copies | Yes | Date of Meeting + 3 years | SHRED | Minutes may contain personal information so default method of disposal is shredding |
| Agendas | No | Permanent - archive one copy with master of minutes, All other copies date of meeting | ARCHIVE one copy. All other copies SHRED | Transfer to archive for permanent retention after 6 years |
| Reports (including annual report) | Yes | Date of report + 6 years. If minutes refer directly to individual report, said report must be kept permanently | ARCHIVE | Dispose of after retention period |
| Annual Parent's Meeting papers | No | Date of meeting + 6 years | SHRED | Dispose of after retention period |
| Instruments of Government including Articles of Association | No | Permanent | Retain in school whilst school is open | Transfer to archive when the school has closed |
| Trusts and Endowments managed by the Governing Body | No | Permanent | Retain in school whilst operationally required | Transfer to archive |
| Action Plans | No | Date of action + 6 years | SHRED | These could be disposed of after 3 years but they are often linked to finances which have to be retained for a minimum of 6 years after the end of the financial year. (especially important if the school has been through a difficult period) |
| Policy Documents | No | Life of policy + 3 years | SHRED | Retained for inspection purposes – important if policy is linked to previous decision making process. Version control important. |

| 2. Governors (continued) | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Complaints files | Yes | Date of resolution of complaint + 6 years | SHRED | Review for further retention before destruction in the case of contentious disputes. Destroy routine complaints. Complaints alleging possible harm to a pupil by a member of staff are covered in 1 above. |
| Annual reports required by the Department for Education | No | Date of report + 10 years | SHRED | Dispose of after retention period |
| Proposals for change of status of a maintained school including specialist status schools and academies | No | Date proposal accepted or declined + 3 years | SHRED | Dispose of after retention period |
| Governor personal details: name, address, date of birth | Yes | Whilst in post + 6 years | ARCHIVE | Keep a record in the Single Central Record. Dispose of after retention period |
| Trustees personal details: name, address, date of birth | Yes | Retained by Companies House on statutory register. Date of appointment + 20 years | ARCHIVE | Keep a record in the Single Central Record. Dispose of after retention period |

| 3. Management | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Log books | Yes | Date of last entry + 6 years | SHRED | May contain personal information |
| Minutes of the Senior Leadership Team and other internal administrative bodies | Yes | Date of meeting + 3 years | SHRED | May contain personal information |
| Records created by Head Teacher or management team (except child protection records which are dealt with in section 1 above) | Yes | Current academic year + 6 years | SHRED | May contain personal information |
| Correspondence created by Head, Deputy Heads, Heads of Year and other members of staff with administrative responsibilities | Yes | Date of correspondence + 3 years | SHRED | May contain personal information |
| Professional Development Plans | Yes | Life of the Plan + 6 years | SHRED | May contain personal information |
| School Development Plans | No | Life of the Plan + 3 years | SHRED | Review before destroying for relevance to any current actions or decisions |
| All records relating to the creation and implementation of School Admissions Policy | No | Life of the policy + 3 years | SHRED | Review before destroying for relevance to any current actions or decisions |
| Admissions if successful | Yes | Admission + 1 year | SHRED | May contain personal information |

| 3. Management (continued) | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Admissions if the appeal is unsuccessful | Yes | Resolution of case + 1 year | SHRED | May contain personal information |
| Proof of address provided by parents as part of the admissions process | Yes | Current + 1 year | SHRED | May contain personal information |
| Supplementary information form including additional information such as medical conditions, religion etc. | Yes | Successful admission – add to the pupil file<br>Unsuccessful admission – until the appeals process is complete | SHRED | May contain personal information |

## 4. Pupils

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Admission registers | Yes | Date of last entry in the book or file + 6 years | SHRED | Review before destroying. Schools may wish to consider keeping admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school |
| Attendance registers | Yes | Date of entry + 3 years | SHRED AND/OR DISPOSAL | If these record are retained electronically any back up copies should be destroyed at the same time |
| Correspondence relating to authorised absence | Yes | Current academic year + 2 years | SHRED | May contain personal information |
| Correspondence relating to unauthorised absence and issues | Yes | Date of absence + 2 years | SHRED | May contain personal information |
| Pupil files retained in school | Yes | Retain for the time the pupil remains at the school | TRANSFER | Transfer to secondary school or other primary school when the child leaves the school. In the case of exclusions it may be appropriate to transfer the record to the Pupil Referral Unit |
| Special Educational Needs files, reviews and IEP's | Yes | DOB of the pupil + 25 years **minimum.** Recommendation is from date of leaving the school/academy, files should be retained for 70 years | SHRED | Review before destroying. **Note**: this retention period is the minimum and some authorities elect to keep SEN files for a longer period<br><br>Special category data MUST be shredded and disposed of securely at the end of its administrative life |
| Any other records created in the course of contact with pupils | Yes | Current academic year + 3 years | SHRED | Review at the end of 3 years and either allocate a further retention period or dispose or shred |
| Child protection information held on pupil file | Yes | If any records relating to child protection are placed on the pupil file, they should be in a sealed envelope and retained for the same period of time as the pupil file | See pupil files above | See pupil files above |

| 4. Pupils (continued) | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Child protection information held in separate files | Yes | Retain for the time the pupil remains at the school.<br><br>*If there is an ongoing investigation by outside agencies the school should retain a copy after the pupil transfers to secondary or other primary school.* | TRANSFER | Transfer to secondary school or other primary school when the child leaves the school.<br><br>In the case of exclusions it may be appropriate to transfer the record to the Pupil Referral Unit.<br><br>Where a child is removed from roll to be educated at home, the file should be transferred to the Local Education Authority.<br><br>Special category data not transferred MUST be shredded and disposed of securely at the end of its administrative life (DOB of the child + 25 years). |
| Statement maintained under the Education Act 1996- Section 234 and any amendments made to the statement | Yes | DOB + 25 years. (This would normally be retained on the pupil file) | SHRED | Shred unless legal action is pending.<br><br>Special category data MUST be shredded and disposed of securely at the end of its administrative life. |
| Advice and information to parents regarding educational needs | Yes | DOB of pupil + 25 years. (This would normally be retained on the pupil file) | SHRED | Shred unless legal action is pending.<br><br>Special category data MUST be shredded and disposed of securely at the end of its administrative life. |
| Accessibility Strategy | Yes | DOB + 25 years. (This would normally be retained on the pupil file) | SHRED | Special category data MUST be shredded and disposed of securely at the end of its administrative life. |
| Parental consent forms for school trips – where there has been no major incident | Yes | Conclusion of the trip | SHRED | May contain personal information |

| 4. Pupils (continued) | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Parental consent forms for school trips – where there has been a major incident | Yes | DOB of the pupil involved in the incident + 25 years. The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils | SHRED | May contain personal information |
| Pupil medical records | Yes | DOB + 25 years | SHRED | Special category data MUST be shredded and disposed of securely at the end of its administrative life. |

| 5. Curriculum | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Curriculum development | No | Current academic year + 6 years | DESTROY | **If personal data is recorded in the records, they must be shredded**. |
| SAT's records | Yes | Current academic year + 6 years | SHRED | May contain personal information |
| Trip records | Yes | Date of trip + 2 years | SHRED | See also H & S with regard to risk assessments. Records should be retained for longer if an incident occurs |
| Pupil's work | No | Current academic year + 1 year | DESTROY | Review these records at the end of each academic year and allocate a new retention period or destroy |
| Class record books | No | Current academic year + 1 year | DESTROY | Review these records at the end of each academic year and allocate a new retention period or destroy**. If additional personal data is recorded in the books, they must be shredded.** |
| Schemes of work | No | Current academic year + 1 year | DESTROY | Review these records at the end of each academic year and allocate a new retention period or destroy |

## 6. Staff Records

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Contracts of employment | Yes | End of contract + 6 years | SHRED | May contain personal information |
| Timesheets | Yes | End of contract + 6 years | SHRED | May contain personal information |
| Personnel files (including leave and training records) | Yes | End of contract + 6 years | SHRED | May contain personal information |
| Interview notes and recruitment records | Yes | Date of interview + 3 years (if successful) | SHRED | See also separate note on retention of DBS certificates.<br><br>Notes from unsuccessful candidates can be destroyed after 6 months |
| Pre-employment vetting information (including unsuccessful DBS checks) | Yes | Date of check + 6 months (if unsuccessful) | SHRED | **If successful**, this information must be placed on the personnel file and managed in line with this policy |
| Pension or other benefit schedule | Yes | Permanent | ARCHIVE | Transfer to archive after employee has left employment |
| Disciplinary proceedings for all matters **except** those relating to child protection issues (for these circumstances see section 1) (Including investigation notes and witness statements) | Yes | **Informal warning**: date of warning + 6 months<br>**Written warnin**g: date of warning + 12 months<br>**Final Warning**: date + 18 months | SHRED | If these are placed on personnel files they need to be removed at the end of the retention period<br><br>**If, following investigation there is found to be no case to answer (except child protection allegations – see section 1), documents should be shredded upon conclusion of the case** |
| Records relating to accident/injury at work | Yes | Date of incident + 5 years | SHRED | Review at the end of this period. In the case of serious accident, a further retention period will need to be applied |

| 6. Staff Records (continued) | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Appraisal documentation and assessment records or action plans | Yes | Duration of employment + 6 years | SHRED | May contain personal information |
| Health records | Yes | Duration of employment + 6 years | SHRED | May contain personal information |
| Pension records | Yes | Last payment + 6 years | SHRED | May contain personal information |
| Salary records | Yes | End of employment + 6 years | SHRED | May contain personal information |

## 7. Health and Safety

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Accessibility plans | Yes | Current year + 6 years | DESTROY | May contain personal information |
| Accident reporting records | Yes | Adults: last entry in the book/file + 4 years<br><br>Children: DOB + 25 years | SHRED | Latent injuries can take years to manifest and the limitation period for claims reflects this. Notes should be kept of all procedures as they were, along with a record that they were followed. Review each case before destruction, especially if a case is live.<br><br>Child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25, this retention period has been applied. |
| COSHH | No | Current year + 10 years | DESTROY | Review and where appropriate an additional retention period may be allocated |
| Policy Statements | No | Date of expiry + 3 years | DESTROY | Version control is important |
| Risk Assessments, including personal RA's | Yes (if personal) | Completion of project, event, incident or activity + 7 years | SHRED | Retain if risk assessment relates to a visit or trip during which an incident occurred and a claim is ongoing. Review if an incident occurred but no claim was made**. Risk assessments for trips can be destroyed 3 years after the trip if no incident occurred** |
| Process of monitoring areas where employees are likely to have come into contact with asbestos | No | Last action + 40 years | DESTROY | Records maintained by Estates Manager |
| Process of monitoring areas where employees are likely to have come into contact with radiation | No | Last action + 50 years | DESTROY | Records maintained by Estates Manager |
| Fire Log Books | No | Current year + 6 years | DESTROY | Records maintained by Estates Manager |

## 8. Administration

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Employers Liability Certificate | No | Permanent | ACHIVE | Retain for 40 years after the school has closed |
| Inventory of furniture and equipment | No | Disposal of last item + 6 years or date superseded + 6 years | DESTROY | |
| School prospectus | No | Current academic year + 3 years | ARCHIVE | Transfer to archive |
| Circulars (staff/parents/pupils) | No | Current academic year + 1 year | DESTROY/ARCHIVE | Review for any items which may be usefully archived |
| Newsletters etc. | Yes | Current academic year + 1 year | SHRED/ARCHIVE | Review for any items which may be usefully archived |
| Visitors' book | Yes | Current academic year + 2 years | SHRED/ARCHIVE | Review for any items which may be usefully archived |
| Insurance Policy | No | End of cover + 1 year | SHRED | May contain confidential Company information |
| Insurance records (renewals, claims, notifications etc) | No | End of cover + 7 years | SHRED | Review before destruction. Retain records for claims which may be ongoing for a further period |

| 9. Finance | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Annual accounts | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| Loans and grants | No | Date of last payment + 12 years | SHRED | May contain confidential Company financial information |
| Contracts | No | Contract completion + 6 years | SHRED | May contain confidential Company financial information |
| Copy orders | No | Current year + 2 years | SHRED | May contain confidential Company financial information |
| Budget reports/monitoring documents | No | Life of the budget + 3 years | SHRED | May contain confidential Company financial information |
| Invoices, receipts and other records covered by the Financial Regulations | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| Annual budget and background papers | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| Delivery documentation | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| Debtor's records | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| School Fund cheque books | No | Current year + 3 years | SHRED | May contain confidential Company financial information |
| School Fund paying in books | No | Current year + 6 years | SHRED | May contain confidential Company financial information |

## 9. Finance (continued)

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| School Fund bank statements | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| School fund ledger, invoices and receipts | No | Current year + 6 years | SHRED | May contain confidential Company financial information |
| Free School Meals registers | Yes | Current year + 6 years | SHRED | May contain personal information.<br><br>Special category data MUST be shredded and disposed of securely at the end of its administrative life |
| Petty cash books | No | Current year + 3 years | SHRED | May contain confidential Company financial information |
| School Meal registers, summaries and records | No | Current year + 3 years | SHRED | May contain confidential Company financial information |
| Bursary/grant applications | No | Current year + 3 years | SHRED | May contain confidential Company financial information |

| 10. Property | | | | |
|---|---|---|---|---|
| **Data Description** | **Data Protection Issues** | **Retention Period** | **Action at the end of the administrative life of the record** | |
| Title deeds | No | Permanent | ARCHIVE | May contain confidential Company information |
| Plans | No | Permanent | ARCHIVE | Retain in school whilst operational |
| Maintenance and contractors records and reports | Yes | Current year + 6 years | SHRED | May contain confidential Company information.<br><br>If personal details about individual contractors are included these must be shredded at the end of their life |
| Service Level Agreements | Yes | Until superseded | SHRED | May contain confidential Company information.<br><br>If personal details about individual contractors are included these must be shredded at the end of their life |
| Leases | No | Expiry of lease + 6 years | SHRED | May contain confidential Company information |
| Lettings | Yes | Current year + 6 years | SHRED | May contain confidential Company information.<br>If this documentation contains personal detail about individuals these must be shredded at the end of their life |
| Burglary, theft and vandalism reports | Yes | Current year + 6 years | SHRED | May contain confidential Company information.<br>If this documentation contains personal detail about individuals these must be shredded at the end of their life |
| Maintenance log books | No | Current year + 6 years | SHRED | May contain confidential Company information.<br>If this documentation contains personal detail about individuals these must be shredded at the end of their life |
| Contractors' reports | No | Current year + 6 years | SHRED | May contain confidential Company information.<br>If this documentation contains personal detail about individuals these must be shredded at the end of their life |

## 11. Local Authority

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Secondary transfer sheets | Yes | Current year + 2 years | SHRED | May contain personal information |
| Attendance returns | Yes | Current year + 1 year | SHRED | May contain personal information |
| Circulars from LA | No | Whilst operationally required | DISPOSE | Review to see whether a further retention period is required before disposal |

## 12. Department for Children, Schools and Families

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| HMI reports | No | No longer need to be retained | SHRED | |
| Ofsted reports | No | Replace former report with any new inspection report | SHRED | Review to see whether a further retention period is required |
| Returns | No | Current year + 6 years | DISPOSE | Review to see whether a further retention period is required before disposal |
| Circulars | No | Whilst operationally required | SHRED | Review to see whether a further retention period is required |

## 13. Work Experience

| Data Description | Data Protection Issues | Retention Period | Action at the end of the administrative life of the record | |
|---|---|---|---|---|
| Work experience and risk assessments | Yes | DOB of child + 18 years | SHRED | |

**APPENDIX B – Data Protection Nominated Representatives**

The nominated representatives in each Extend Learning Academies Network school, with contact details are listed below.

| | |
|---|---|
| Central Team | Karen Romano (Data Protection Officer) 01934 427136 |
| Bournville Primary School | Rachel Thomas 01934 427130 |
| Locking Primary School | Kimberley Underhill 01934 822867 |
| Mead Vale Primary School | Nicola Bignell 01934 511133 |
| Mendip Green Primary School | Amanda Shipton 01934 513791 |
| Milton Park Primary School | Rebecca Perry 01934 624868 |
| Oldmixon Primary School | Lesley Newson 01934 812879 |
| Walliscote Primary School | Mandy Davies 01934 621954 |
| Windwhistle Primary School | Miesha Vowles 01934 629145 |