DATA PROTECTION POLICY 2018
In accordance with GDPR regulations

THIS POLICY APPLIES TO THE TRUST BOARD, ALL TRUST SCHOOLS AND THE HOPE TEACHER TRAINING PARTNERSHIP

Document Management:
Date Policy Created: March 2018
Date Policy Approved: 23 May 2018
Date Amended:
Next Review Date: April 2019
Version: 2.0
Approving Body: Full Trust Board

Contents:

Statement of intent

Hope Learning Trust York 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).

For the purposes of this document, the "Trust" refers to the Hope Central Team, the Trust Board, Trust Members, All Trust Schools, and the Hope Teacher Training Partnership (Ebor Teaching Schools Alliance).

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

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

Organisational methods for keeping data secure are imperative, and **Hope Learning Trust York** 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:

_____ Chief Executive Officer Date: _____

_____ Chair of Trustees Date: _____

1. Legal framework

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

- The General Data Protection Regulation (GDPR)
- The Data Protection Bill 2017
    - 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 to the following guidance:

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

1.3. This policy will be implemented in conjunction with the following other Trust/Academy documents:

- HLTY Photography and Videos at School Policy
- HTLY E-Security Policy
- HLTY Freedom of Information Policy
- HLTY CCTV (Model) Policy – Individual Academies'
- HLTY 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.

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. **Hope Learning Trust York** 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 Trust will provide comprehensive, clear and transparent privacy policies.

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

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 Trust 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 Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's and all of its schools' 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 in the Trust, which is the Trust Board.

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 Trust 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 based on 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 based on 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 Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

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 years, 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 regarding 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 Trust 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 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 Trust 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 Trust 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 Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5. Where a SAR has been made verbally, the individual will be required to put the request in writing (an email will suffice).

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

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

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

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

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

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

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

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 Trust will inform them of the rectification where possible.

10.3. Where appropriate, the Trust 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 Trust 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 Trust 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 Trust 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 Trust's processing of personal data.

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

13.9. The Trust 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 Trust 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 Trust 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 Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust 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 Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust 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 Trust 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 Trust 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 Trust 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 Trust 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 Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest based on Union/Member State law.

16. Privacy by design and privacy impact assessments

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

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

16.3. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust'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 Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

16.8. Where a DPIA indicates high risk data processing, the Trust 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/Principal 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 Trust 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 Trust 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 Trust, 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 Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8. Staff may **NOT** use personal (i.e. owned by the member of staff) laptops, smartphones, computers, tablets, hard drives or other devices for Trust purposes, including accessing school or Trust email accounts and downloading documents. Use of personal devices for school/Trust purposes outside of school premises is also prohibited.

18.9. Governors, Trustees and Members who use personal devices for Trust purposes to access school or Trust email accounts agree to download or print documents **only as necessary**; any hard copies of Trust documents must be brought to the Hope Offices for secure disposal once no longer required. Electronic copies must be securely deleted from any private device including any metadata relating to the document. Emails containing personal data will be deleted once no longer required for the initial purpose.

18.10. All necessary members of staff, Governors and Trustees are provided with their own secure login and password, and every computer regularly prompts users to change their password.

18.11. All necessary Governors, Trustees and Members will be given access to relevant school or Trust documents via secure remote access; these documents must be downloaded or printed only as necessary; any hard copies of these documents must be brought to the relevant school/Hope Offices for secure disposal. Electronic copies must be securely deleted from any private device including any metadata relating to the document.

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

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

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

18.15. 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.

18.16. 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.

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

18.18. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.19. **Hope Learning Trust York** takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.20. The **designated individual** is responsible for continuity and recovery measures are in place to ensure the security of protected data. Named members of staff at each establishment are provided in **Appendix B.**

19. Publication of information

19.1. **Hope Learning Trust York** publishes on its website 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. **Hope Learning Trust York** 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 website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV and Photography

20.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles, as outlined in each Trust school's CCTV Policy.

20.2. The Trust 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 **three days** for security purposes; the **Operations Director** is responsible for keeping the records secure and allowing access.

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

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

20.7. Precautions, as outlined in the **Photography and Videos at School Policy**, are taken when publishing photographs of pupils, in print, video or on the school 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 Trust 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.

21.5. Data Retention periods are outlined in the Data Retention Schedule (Appendix A).

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 annually by the Data Protection Officer and the Operations Director.

The next scheduled review date for this policy is **April 2019**

1 Child Protection

	Basic File Description	Data Prot Issues	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
1.1	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education" September 2004	DOB + 25 years To be advised – 50 years after pupil leaves school/academy	SECURE DISPOSAL
1.2	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. Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005.	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer. Note allegations that are found to be malicious should be removed from personnel files.	SECURE DISPOSAL These records must be shredded.

2 Governors

GOVERNORS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
2.1	Minutes				
2.2	Principal Set (signed)	Yes		PERMANENT	If school unable to store these, they should be offered to County Archives Service.
2.3	Inspection copies [1]	Yes		Date of meeting + 3years	SECURE DISPOSAL (If these minutes contain any sensitive personal information they should be shredded)
2.4	Agendas	No		Once copy retained with master of minutes. All other copies: Date of Meeting	SECURE DISPOSAL
2.5	Reports Presented to the Governing body	Yes		Date of Report + 6 years. If minutes refer directly to individual report, said reports must be kept permanently	SECURE DISPOSAL or retain with signed set of minutes
2.6	Annual Parents' meeting papers	No	Education Act 2002, Section 33	Date of meeting + 6 years (min)	SECURE DISPOSAL
2.7	Instruments of Government incl Articles of Association	No		PERMANENT	Retain in school whilst school is open, then offered to County Archives
2.8	Trusts and Endowments managed by governing body	No		PERMANENT	Retain in school whilst operationally required then offered to County Archives
2.9	Action Plans	No		Date of Action Plan + 3 years	SECURE DISPOSAL

GOVERNORS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
2.10	Policy Documents	No		Life of Policy + 3 years	SECURE DISPOSAL
2.11	Complaints Files	Yes		Date of Resolution of complaint + 6 years (min) Review for further retention in the case of contentious disputes	SECURE DISPOSAL routine complaints
2.10	Annual reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002 SI2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
2.11	Proposals for change of status of a maintained school including Specialist status schools and academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL
	Governor personal details: Name, address, date of birth	Yes			
2.	Trustees personal details, name, address and date of birth	Yes		Retained by Companies house on statutory register Date of appointment + 20 years	ARCHIVED
3.					

[1] These are copies which the clerk to governors may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

3 Management

MANAGEMENT					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
3.1	Log Books	Yes		Date of last entry in the book + 6 years	Could be offered to County Archives Service if appropriate
3.2	Minutes of the Senior Management team and other internal administrative bodies	Yes		Date of Meeting + 3 years	SECURE DISPOSAL
3.3	Reports made by the head teacher or the management team	Yes		Date of report + 3 years	SECURE DISPOSAL
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Current academic year + 6 years the review	SECURE DISPOSAL
3.5	Correspondence created by head teachers deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Date of correspondence + 3 years then review	SECURE DISPOSAL
3.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
3.7	School Development plans	No		Life of the Plan + 3 Years	SECURE DISPOSAL
3.8	All records relating to the creation and implementation of School Admissions policy	No	School Admissions Code Dec 2014	Life of the Policy + 3 years then review	SECURE DISPOSAL
3.9	Admissions – If the admission is successful	Yes	School Admissions Code Dec 2014	Admission + 1 year	SECURE DISPOSAL

MANAGEMENT					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
3.10	Admission – if the appeal is unsuccessful	Yes	School Admissions Code Dec 2014	Resolution of case + 1 year	SECURE DISPOSAL
3.11	Register of Admission	Yes	School Attendance: Departmental Advice Oct 2014 (p.6)	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	REVIEW 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
3.12	Admissions – Secondary Schools Casual	Yes		Current Year + 1 year	SECURE DISPOSAL
3.13	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Dec 2014	Current year + 1 year	SECURE DISPOSAL
3.14	Supplementary information form including additional information such as religion, medical conditions etc.	Yes			
3.15	• For successful admissions	Yes		Information should be added to pupil file	SECURE DISPOSAL
3.16	• For unsuccessful admissions	Yes		Until Appeals process completed	SECURE DISPOSAL

4 Pupils

PUPILS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
4.1	Admissions Registers	Yes		Date of last entry in the book (or file) + 6 yrs	Retain in school for 6 years from date of last entry then consider transfer to Archives
4.2	Attendance registers	Yes	School Attendance: Departmental advice for maintained schools, academies, independent schools and local authorities Oct 2014	Date of entry + 3 years	SECURE DISPOSAL (If these records are retained electronically any back up copies should be destroyed at the same time)
4.3	Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL
4.4	Pupil files retained in Schools	Yes	The Education (Pupil Information) Regulations 2005 SI 2005 No 1437		
4.4.1	• Primary			Retain for the time which the pupil remains at the Primary School	Transfer to secondary school or other primary school when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit
4.4.2	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years [1]	SECURE DISPOSAL
4.5	Special Educational Needs Files, reviews and IEPs	Yes	Limitation Act 1980 (Section 2)	DOB of the Pupil + 25 years min (recommendation is from date of leaving the school/academy, files should be retained for 70 years)	REVIEW Note: This retention period is the minimum; some authorities choose to keep SEN files for a longer period

PUPILS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
					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.
4.6	Correspondence relating to Authorised Absence and Issues	No		Date of absence + 2years	SECURE DISPOSAL
4.7	Examination results	Yes			

PUPILS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
4.7.1	• Public	Yes		Added to pupil file	All uncollected certificates should be returned to the examination board
4.7.2	• Internal examination results	Yes		Added to pupil file	SECURE DISPOSAL
4.8	Any other records created in the course of contact with pupils	Yes		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
4.9	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
4.10	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 working to safeguard and promote	DOB of the child + 25 years then review. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that	SECURE DISPOSAL – These records MUST be shredded

PUPILS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
			the welfare of children March 2015.	the principal copy of this information will be found on the LA Social Services Record	
4.11	Statement maintained under The Education Act 1996 – Section 234 and any amendments made to statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DOB + 25 years (This would normally be retained on the pupil file)	SECURE DISPOSAL unless legal action is pending
4.12	Advice and information 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 legal action is pending
4.13	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	DOB + 25 years (This would normally be retained on the pupil file)	SECURE DISPOSAL unless legal action is pending
4.14	Parental consent forms for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
4.15	Parental consent forms for school trips – where there has been no major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The Permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL

PUPILS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
4.16	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 http://oeapng.info specifically Section 3 – " Legal Framework and Employer Systems" and Section 4 – "Good Practice"	Date of visit + 14 years [3]	SECURE DISPOSAL
4.17	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 http://oeapng.info specifically Section 3 – " Legal Framework and Employer Systems" and Section 4 – "Good Practice"	Date of visit + 10 years	SECURE DISPOSAL
4.18	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)

[2] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.
[3]This retention period has been set in agreement with Safeguarding Children's Officer.

5 Curriculum

CURRICULUM					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
5.4	Timetable	No		Current year + 1 year	
5.5	Class record books	No		Current year + 1 year	
5.6	Mark Books	No		Current year + 1 year	
5.7	Record of homework set	No		Current year + 1 year	
5.8	Pupils' work	No		Current year + 1 year	
5.9	Examination results	No		Current year + 6 years	SECURE DISPOSAL
5.10	SATS records	Yes			

CURRICULUM					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
5.10.1	• SATS results	Yes		SATs results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison.	SECURE DISPOSAL
5.10.2	• Examination papers	Yes		The examination papers should be kept until any appeals/validation process is complete.	SECURE DISPOSAL
5.11	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
5.13	Self Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6 Personnel Records

PERSONNEL RECORDS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
6.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
6.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
6.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All relevant information should be added to personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
6.4	Interview notes and recruitment notes	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.5	Pre-employment vetting information (including DBS checks)	Yes	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory guidance from DfE) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so, the copy must NOT be retained for more than 6 months	SECURE DISPOSAL (by designated member of staff)
6.6	Proofs of identity collected as part of the process of checking 'portable' enhanced CRB disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation, then this should be placed on the	SECURE DISPOSAL

PERSONNEL RECORDS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
				staff's personal file?? Passport copies kept? ?	
6.7	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom [4]	Yes	An Employer's Guide to Right to Work Checks (Home Office May 2015)	Where possible these documents should be added to the Staff personnel File (see below) but if they are kept separately then the home office requires that the documents are kept for termination of Employment plus not less than two years	
6.8	Timesheets, sick pay	Yes	Financial regulations	Current year + 6 years	SECURE DISPOSAL
6.9	Staff Personal files	Yes	Limitation Act 1980 (Section 2)	Termination + 6 years	SECURE DISPOSAL
6.10	Disciplinary proceedings	Yes	Where the warning relates to a child protection issue see 1.2 and see safeguarding children officer for further advice		

PERSONNEL RECORDS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
6.10.1	• Oral warning	Yes		Date of warning + 6 months	SECURE DISPOSAL If warnings are placed on a personal file they must be weeded from the file
6.10.2	• Written warning – level one	Yes		Date of warning + 6 months	
6.10.3	• Written warning – level two	Yes		Date of warning + 12 months	
6.10.4	• Final warning	Yes		Date of warning + 18 months	
6.10.5	• Case not found	Yes		If child protection related see 1.2 otherwise SECURE DISPOSAL	SECURE DISPOSAL immediately at the conclusion of the case
6.11	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
6.12	Annual appraisal/assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
6.13	Salary cards?	Yes		Date of last employment + 85 years	SECURE DISPOSAL
6.14	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) revised 1999 (SI 1999/567)	Current year + 3 years	SECURE DISPOSAL
6.15	Records held under Retirement Benefits Schemes (information powers) regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

7 Health and Safety

HEALTH AND SAFETY					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
7.1	Policy statements	No		Date of expiry + 1 year	SECURE DISPOSAL
7.2	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.3	Records relating to accident/injury at work (Also see Personnel Records above)	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be applied	SECURE DISPOSAL
7.4	Accident Reporting	Yes	Social Security (Claims and Payments) regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.4.1	• Adults			Date of the incident + 6 years	SECURE DISPOSAL
7.4.2	• Children			DOB of child + 25 years	SECURE DISPOSAL
7.5	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
7.6	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

HEALTH AND SAFETY					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
7.7	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
7.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL
7.9	Workplace Inspections	No		Current year + 3 years	SECURE DISPOSAL

8 Administrative

ADMINISTRATIVE					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
8.1	Employer's Liability Insurance certificate	No		Closure of school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment and furniture	No		Current year + 6 years	SECURE DISPOSAL
8.3	General file series	No		Current year + 5 years then review	Review to see whether a further retention period is required
8.4	School brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
8.5	Circulars (Staff/parents/pupils)	No		Current year + 1 year	STANDARD DISPOSAL
8.6	Newsletters, etc.	No		Current year + 1 year	STANDARD DISPOSAL
8.7	Visitors' book/Signing in Sheetss	Yes		Current year + 6 years then review	SECURE DISPOSAL
8.8	PTA/Old Pupils Associations	No		Current year + 6 years	SECURE DISPOSAL

9 Finance

FINANCE					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
9.1	Annual accounts	No		Current year + 6 years	STANDARD DISPOSAL
9.2	Loans and Grants	No		Date of last payment on loan + 12 years	SECURE DISPOSAL
9.3	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
9.4	Invoices, receipts, order books, requisitions and delivery notices	No	Financial Regulations	Current financial year + 6 years	SECURE DISPOSAL
9.5	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
9.6	Debtors' Records		Limitation Act 1980	Current financial year + 6 years	SECURE DISPOSAL
9.7	Contracts				SECURE DISPOSAL
9.7.1	• Under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
9.7.2	• Under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
9.7.3	• Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
9.8	School fund – cheque books	No		Current year + 6 years	SECURE DISPOSAL

FINANCE					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
9.9	School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
9.10	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
9.11	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
9.12	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
9.13	School fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL
9.14	School Fund – school journey books	No		Current year + 6 years	SECURE DISPOSAL
9.15	Student Grant applications	Yes		Current + 3 years	SECURE DISPOSAL
9.16	Free School Meals Registers	Yes		Current year + 6	SECURE DISPOSAL
9.17	School Meal Registers	Yes		Current + 3 years	SECURE DISPOSAL
9.18	School Meal summary sheets	No		Current + 3 years	SECURE DISPOSAL
9.19	Petty cash books	No		Current + 6 years	SECURE DISPOSAL

10 Property

PROPERTY					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
10.1	Title Deeds	No		PERMANENT these should follow the property unless the property has been registered at the Land Registry	PERMANENT

PROPERTY					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
10.2	Plans of property	No		Permanent	Retain in school whilst operational
10.3	Maintenance and contractors	No	Financial Regulations	Current Year + 6 years	SECURE DISPOSAL
10.4	Leases	No		Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 6 years	SECURE DISPOSAL
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance Log books			Current year + 6 years	SECURE DISPOSAL
10.8	Contractors' reports			Current year + 6 years	SECURE DISPOSAL

11 Local Authority

LOCAL AUTHORITY					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required

12 Department for Children, Schools and Families

DEPARTMENT FOR CHILDREN, SCHOOLS AND FAMILIES					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
12.1	HMI reports			Do not need to be kept any longer	
12.2	OFSTED reports and papers		DfE? Ofsted?	Replace former report with any new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current Year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, schools and families			Whilst operationally required	Review to see whether a further retention period is required

13 Contracts/Service Level Agreements

CONTRACTS/SERVICE LEVEL AGREEMENTS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work experience agreement			DOB of child + 18 years	SECURE DISPOSAl

14 School Meals

SCHOOL MEALS					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL

15 Family Liaison Officers and Home School Liaison Assistants

Family Liaison Officers and Home school Liaison Assistants					
	Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL
15.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school, then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		Whilst the referral is current	SECURE DISPOSAL
15.4	Contact data sheets	Yes		Current year, then review – if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year, then review – if contact is no longer active then destroy	SECURE DISPOSAL (DELETE INCLUDING ALL BACKUPS)
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

APPENDIX B – Data Protection Nominated Representatives

The nominated representatives in each Hope Learning Trust York school, with contact details are listed below.

Hope Learning Trust	Wendy Munro (DPO)	01904 560053
Manor Church of England Academy	Carol Rowbotham	01904 798722
Vale of York Academy	Vanessa Smallwood	01904 560000
Barlby High School	Vanessa Smallwood	01757 706161
Poppleton Ousebank Primary School	Judy Sandilands	01904 795930
Forest of Galtres Anglican Methodist Primary School	Holly Newby	01904 470272
Burton Green Primary School	Sarah Brownhill	01904 552380