Policies

Data Protection Policy & Procedure

Next review date: July 2026

Contents

1 Introduction and definitions

1.1 Introduction

This Policy sets out the obligations of Holmes Chapel Comprehensive School (HCCS) regarding data protection and the rights of, inter alia, students, parents, staff and visitors ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 (the Act).

This Policy sets the School's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the School, its employees, agents, contractors, or other parties working on behalf of the School.

The School is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and School of all individuals with whom it deals.

1.2 Definitions

The terms in this document have the meanings as set out in Article 4 of the GDPR unless amended by the Act.

For clarity, the following have been reproduced:

'**personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. For the purposes of this policy, Holmes Chapel Comprehensive School is the data controller.

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'special category personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2 The Data protection principles

This Policy aims to ensure compliance with the Act including the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 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.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject.

2.6 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.

2.7 The controller shall be responsible for, and be able to demonstrate compliance with the above principles ('accountability').

3 The rights of data subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12):

3.2 The right of access (Part 13):

3.3 The right to rectification (Part 14):

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15):

3.5 The right to restrict processing (Part 16):

3.6 The right to data portability (Part 17):

3.7 The right to object (Part 18); and

3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4 Lawful, fair, and transparent data processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them:

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject:

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person:

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category personal data" (sometimes referred to as "sensitive personal data") processing is prohibited, unless one, or more, of the following exemptions applies

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or UK law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or UK Law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent:

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject:

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity:

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4.3 Where special category personal data is processed the School shall have both a legal basis from Article 6 for using that personal data and at least one of the exemptions from Article 9(2) shall apply.

5 Specified, explicit and legitimate purposes

5.1 The School collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The School only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the School uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6 Adequate, Relevant, and Limited Data Processing

The School will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7 Accuracy of data and keeping data up to date

7.1 The School shall take all reasonable steps to ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8 Data retention

8.1 The School shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the School's approach to data retention, including retention periods for specific personal data types held by the School, please refer to Appendix 1 of this Policy.

9 Secure Processing

The School shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10 Accountability and record keeping

10.1 The School's Data Protection Officer is GDPR Sentry Limited.

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the School's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 The School shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the School, its Data Protection Officer, and any applicable third-party data processors:

10.3.2 The purposes for which the School collects, holds, and processes personal data:

10.3.3 Details of the categories of personal data collected, held, and processed by the School, and the categories of data subject to which that personal data relates:

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards:

10.3.5 Details of how long personal data will be retained by the School (please refer to the School's Data Retention Policy in Appendix 1); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the School to ensure the security of personal data.

11 Data protection impact assessments

11.1 The School shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed:

11.2.2 The purpose(s) for which personal data is to be used:

11.2.3 The School's objectives:

11.2.4 How personal data is to be used:

11.2.5 The parties (internal and/or external) who are to be consulted:

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed:

11.2.7 Risks posed to data subjects:

11.2.8 Risks posed both within and to the School; and

11.2.9 Proposed measures to minimise and handle identified risks.

12 Keeping data subjects informed

12.1 The School shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the School including, but not limited to, the identity of its Data Protection Officer:

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing:

12.2.3 Where applicable, the legitimate interests upon which the School is justifying its collection and processing of the personal data:

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed:

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties:

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

12.2.7 Details of data retention:

12.2.8 Details of the data subject's rights under the GDPR:

12.2.9 Details of the data subject's right to withdraw their consent to the School's processing of their personal data at any time:

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR):

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13 Data subject access requests

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the School holds about them, what it is doing with that personal data, and why. They are encouraged to make these requests by emailing DPA@hccs.info.

13.2 Employees wishing to make a SAR should contact The Data Protection Team

13.3 Responses to SARs shall normally be made within one calendar month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 Responses to SARs shall be dependent upon the terms of the GDPR, the Data Protection Act (2018) and associated ICO guidance.

13.5 The School does not charge a fee for the handling of normal SARs. The School reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13.6 The School has defined a process for handling SARs and other data subject requests. This process is found in Appendix 2 of this document and is mandatory for all staff.

14 Rectification of personal data

14.1 Data subjects may have the right to require the School to rectify any of their personal data that is inaccurate or incomplete.

14.2 Where such rectification is possible, the School shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the School of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15 Erasure of personal data

15.1 Data subjects have the right to request that the School erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the School to hold that personal data with respect to the purpose(s) for which it was originally collected or processed

15.1.2 The data subject wishes to withdraw their consent to the School holding and processing their personal data:

15.1.3 The data subject objects to the School holding and processing their personal data (and there is no overriding legitimate interest to allow the School to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully:

15.1.5 The personal data needs to be erased in order for the School to comply with a particular legal obligation; or

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 Unless the School has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16 Restriction of personal data processing

16.1 Data subjects may request that the School restricts processing the personal data it holds about them. If a data subject makes such a request, the School shall, in so far as it is possible, ensure that the personal data is only stored and not processed in any other fashion.

16.2 If the School is required to process the data for statutory purposes or for reasons of legal compliance, then the School shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

16.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17 Data portability requests

17.1 The School processes personal data using automated means. Such processing is carried out by, inter alia, our management information system, our human resources system and our catering management system.

17.2 Where data subjects have given their consent to the School to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the School and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18 Objections to personal data processing

18.1 Data subjects have the right to object to the School processing their personal data where such processing is based on the performance of a public task or the legitimate interests of the School which include direct marketing and profiling.

18.2 Where a data subject objects to the School processing any such personal data the School shall act as though the data subject has submitted a request for restriction of processing for the specified personal data

18.3 The School shall be responsible for reviewing the processing the data subject has objected to so as to provide a compelling demonstration of School's grounds for the processing that override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.4 Where a data subject objects to the School processing their personal data for direct marketing purposes, the School shall cease such processing immediately.

18.5 Where a data subject objects to the School processing their personal data for scientific and/or historical research and statistics purposes, the data subject may object on grounds relating to his or her particular situation. The School is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19 Automated decision making

19.1 Data subjects have the right not to be subject to a decision based on automated processing of their personal data, including profiling, where that decision has a legal effect or significantly affects them.

19.2 The School may use such processing if the decision:

19.2.1 is necessary for entering into, or performance of, a contract between the data subject and a data controller:

19.2.2 is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

19.2.3 is based on the data subject's explicit consent.

19.3 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the School.

19.4 Such decisions should not concern a child (natural persons under the age of 18) unless there is a compelling, demonstrated and documented reason for doing so.

20 Profiling

20.1 The School uses personal data for profiling purposes. These purposes relate to helping students maximise achievement and attendance.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling:

20.2.2 Appropriate mathematical or statistical procedures shall be used:

20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21 Personal data collected, held and processed

The School uses a wide range of personal data across many processes. More detail can be found in our Privacy Notices. Our Data Protection Officer can provide a list of the categories of personal data we process.

22 Data security – Transferring personal data and communications

22.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not

permitted in any circumstances:

22.2 The School will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

22.3 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data:

22.4 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

22.5 Where personal data is to be transferred in removal storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the School

23 Data security – Storage

The School shall ensure that the following measures are taken with respect to the storage of personal data:

23.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption:

23.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar:

23.3 All personal data relating to the operations of the School, stored electronically, should be backed up on a regular basis

23.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the School. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information

24 Data security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the School's Data Retention Policy as found in Appendix 1 of this document

25 Data security – Use of personal data

The School shall ensure that the following measures are taken with respect to the use of personal data:

25.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the School requires access to any personal data that they do not already have access to, such access should be formally requested from

25.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the School or not, without the initial authorisation of the Data Protection Lead.

25.3 Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time:

25.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

25.5 Where personal data held by the School is used for marketing purposes, it shall be the responsibility of The Data Protection Team to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26 Data security – IT security

Full details of the School's IT security requirements and procedures can be found in the IT Security Policy. The School shall ensure that, inter alia, the following measures are taken with respect to IT and information security:

26.1 The School requires that any passwords used to access personal data shall have a minimum of 8 characters for google and 6 for the network, composed of a mixture of upper- and lower-case characters, numbers and symbols. Passwords are not expected to be changed upon a regular basis, but users will be expected to change their password if instructed by the School:

26.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the School, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords:

26.3 All software (including, but not limited to, applications and operating systems) shall be kept up to date. The School's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

26.4 No software may be installed on any School-owned computer or device without the prior approval of the IT Manager.

26.5 Where members of staff or other users use online applications that require the use of personal data, the use of that application must be signed off by Data Protection Lead.

27 Organisational measures

The School shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

27.1 All employees, agents, contractors, or other parties working on behalf of the School shall be made fully aware of both their individual responsibilities and the School's responsibilities under the GDPR and under this Policy, and shall have free access to a copy of this Policy;

27.2 Only employees, agents, sub-contractors, or other parties working on behalf of the School that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the School;

27.3 All employees, agents, contractors, or other parties working on behalf of the School handling personal data will be appropriately trained to do so:

27.4 All employees, agents, contractors, or other parties working on behalf of the School handling personal data will be appropriately supervised:

27.5 All employees, agents, contractors, or other parties working on behalf of the School handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

27.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed:

27.7 All personal data held by the School shall be reviewed periodically, as set out in the School's Data Retention Policy:

27.8 The performance of those employees, agents, contractors, or other parties working on behalf of the School handling personal data shall be regularly evaluated and reviewed:

27.9 The contravention of these rules will be treated as a disciplinary matter.

27.10 All employees, agents, contractors, or other parties working on behalf of the School handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract:

27.11 All agents, contractors, or other parties working on behalf of the School handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the School arising out of this Policy and the GDPR; and

27.12 Where any agent, contractor or other party working on behalf of the School handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the School against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28 Transferring personal data to a country out of the EEA

28.1 The School may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

28.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data:

28.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum); standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

28.2.3 The transfer is made with the informed consent of the relevant data subject(s):

28.2.4 The transfer is necessary for the performance of a contract between the data subject and the School (or for pre-contractual steps taken at the request of the data subject):

28.2.5 The transfer is necessary for important public interest reasons:

28.2.6 The transfer is necessary for the conduct of legal claims:

28.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

28.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29 Data breach notification

29.1 All personal data breaches must be reported immediately to the School's Data Protection Officer.

29.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

29.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29.4 Data breach notifications shall include, a minimum, the following information:

29.4.1 The categories and approximate number of data subjects concerned:

29.4.2 The categories and approximate number of personal data records concerned:

29.4.3 The name and contact details of the School's data protection officer (or other contact point where more information can be obtained);

29.4.4 The likely consequences of the breach:

29.4.5 Details of the measures taken, or proposed to be taken, by the School to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29.5 The School has a detailed policy for managing personal data breaches which can be found as Appendix 3 to this document.

30 Implementation of policy

This Policy shall be deemed effective on **7th** December 2020 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

31 Data Protection Officer

The Data Protection Officer for the School is GDPR Sentry Limited.

32 Appendices

Appendix 1: Data retention and disposal policy

Appendix 2: Data subject request policy

Appendix 3: Data breach policy

Prepared by: Neil Barnett
Agreed by the Board To be reviewed annually Date for review: June 2026

Appendix 1: Data retention and disposal policy

1.1 Application

This Policy sets out the measures adopted by referred to as "we" or "our") in respect of the retention and disposal of records that contain personal data or other confidential information.

1.2 Purpose

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents.

1.3 Review

Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

1.4 How long should we keep our records

Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements. We have assessed our records to:

- Determine their value as a source of information about the School, its operations, relationships and environment
- Assess their importance as evidence of business activities and decisions
- Establish whether there are any legal or regulatory retention requirements (including: Public Records Act (1958), the Freedom of Information Act (2000), the Limitation Act (1980), the Data Protection Act (2018).

Where records are likely to have a historical value, or are worthy of permanent preservation, we may choose to archive them at the end of any statutory retention period.

1.5 Disposal schedule

A disposal schedule is a key document in the management of records and information. It is a list of series or collections of records for which predetermined periods of retention have been agreed between School and the DPO.

Records on disposal schedules will fall into three main categories:

- Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 3 years; destroy 2 years after the end of the financial year).
- Automatically select for permanent preservation – where certain groups of records can be readily defined as worthy of permanent preservation and transferred to an archive.
- Review – unknown at present but subject to review in a defined period of time see 3 above.

1.6 Records can be destroyed in the following ways:

- Non-sensitive information – can be placed in a normal rubbish bin
- Confidential information – crosscut shredded and pulped or burnt
- Highly Confidential information – crosscut shredded and pulped or burnt
- Electronic equipment containing information - destroyed using Killdisc or equivalent technology and for individual folders, they will be permanently deleted from the system.

Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

The Disposal Schedule will be kept up to date in that new categories of data are added

1.7 Data sharing and disposal

Where we share information with other bodies, we will ensure that they have adequate procedures for data retention and disposal to ensure that the information is managed in accordance with the School ’s policies, relevant legislation and regulatory guidance.

Where relevant to do so we will carry out a data protection impact assessment and update our privacy notices to reflect data sharing.

1.8 Record-Keeping

It is not necessary to document the disposal of records when that has been done in line with the records retention schedule. Documents disposed of outside the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.

This will provide an audit trail for any inspections conducted by the Information Commissioner’s Office and will aid in addressing Freedom of Information requests, where we no longer hold the material.

1.9 Monitoring

Responsibility for monitoring the disposal policy rests with the School’s Data Protection Lead. The policy will be reviewed annually or more often if required.

Appendix 2 Records retention schedule

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a crosscut shredder.

These are the copies which the clerk to the Governor 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.

1.1 Governing Body					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	School s and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

	school including Specialist Status Schools and Academies				

Please note that all information about the retention of records concerning the recruitment of Headteachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Logbooks of activity in the school maintained by the Head Teacher	There may be data protection issues if the logbook refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL

1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

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

	Schools – Casual				
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

1.3 Admissions Process					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL

1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

2.1 Recruitment					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) 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	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS 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 member of staff's personal file	

2.1.6	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 Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.3 Management of Disciplinary and Grievance Processes					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and School s March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	

					from the file]
	case not found			If the incident is child protection related, then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

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

2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions logbooks	No		Current year + 6 years	SECURE DISPOSAL

2.5 Payroll and Pensions					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

Risk Management

3.1 Risk Management and Insurance					
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
Basic file description		Data Prot	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

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

3.4 Contract Management					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund					
Basic file description the Issues		Data Prot Provisions	Statutory	Retention Period [Operational]	Action at the end of administrative life of the record
3.5.1	School Fund - Cheque books		No	Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books		No	Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger		No	Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices		No	Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts		No	Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements		No	Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books		No	Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management					
Basic file description the Issues		Data Prot Provisions	Statutory	Retention Period [Operational]	Action at the end of administrative life of the record
3.6.1	Free School Meals Registers		Yes	Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers		Yes	Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets		No	Current year + 3 years	SECURE DISPOSAL

Premises

4.1 Property Management					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased	No		Expiry of lease + 6 years	SECURE DISPOSAL

	by or to the school				
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance logbooks	No		Current year + 6 years	SECURE DISPOSAL

5.1 Pupil's Educational Record					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the

					normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

2 **Pupil Information**

5.1 Pupil's Educational Record				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3 Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance	If any records relating to child protection issues are placed on the pupil	SECURE DISPOSAL – these records MUST be shredded

			for schools and School s March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and School s March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

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

5.3 Special Educational Needs					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on	SECURE DISPOSAL unless the document is subject to a legal hold

				the pupil file]	
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The 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
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	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
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	

6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7.1 Educational Visits outside the Classroom

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by

					the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

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

7.3 Family Liaison Officers and Home School Liaison Assistants					
Basic file description		Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	

7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority

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

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

Appendix 2: Data subject request policy

1. Purpose

Holmes Chapel Comprehensive school (HCCS) is required to follow the Data Protection Act (2018) (the Act) in the way that it collects and uses personal data. The Act references and implements the General Data Protection Regulation (GDPR) with some specific amendments.

Chapter 3 of the GDPR sets out the rights of data subjects with respect to their personal data. Although the most common right is Subject Access, there are many others. As a group these referred to as 'data subject requests: The regulations set out the steps that data controllers need to put in place to allow data subjects to exercise these rights.

This policy sets out the approach that the School will take to deal with data subject requests. This policy applies to:

- All employees of School
- Governors

The Data Protection Officer is GDPR Sentry Limited.

2 Introduction

The GDPR describes the responsibilities that organisations have when dealing with personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as a 'data subject'.

The GDPR provides data subjects with rights in respect of their personal data. Not all rights apply in respect of all personal data. Data subjects have the following rights:

- Right of access by the data subject
- Right of rectification
- Right of erasure ('right to be forgotten')
- Right of restriction of processing
- Right of data portability
- Right to object to processing
- Right not to be subject to automated individual decision making, including profiling

The nature of the personal data and the reason for its use determine which of these rights are applicable. Guidance about whether a particular right is applicable should be sought from the Data Protection Officer.

When a data subject seeks to exercise one of these rights it is called a data subject request. The most common data subject request is a subject access request (SAR)

As the School deals with young people, there are certain circumstances where a parent or another legal representative may exercise these rights on behalf of the young person. Any situation where there is a question over rights to access personal data or the exercising of these other rights must be referred to the Data Protection Officer.

3 Related policies

This policy is closely linked with other policies which should be referenced when appropriate, including:

- Data Protection Policy
- Child protection
- Safeguarding
- Any other relevant guidance documents

4 Responsibilities

The School will:

Put in place a clear procedure for dealing with data subject requests. This procedure should take account of the requirements laid down in Annex 1.

Follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy

Inform the Data Protection Officer of all data subject requests

Record the details of data subject requests and make those records available to the Data Protection Officer

Ensure that data subject requests are dealt with in line with the statutory time limits and notify the Data Protection Officer as soon as possible if these limits can't be met

Ensure that proper account is taken of the risk of disclosing information about a third party in responding to a data subject request and the risk of failing to maintain the availability and integrity of the personal data it processes.

Take advice from the Data Protection Officer with regards to the management of data subject requests

The Data Protection Officer will:

Provide guidance and support to the School in dealing with a data subject requests

Provide a route of communication to the Information Commissioner's Office in the event of issues with the content or timing of responses to a data subject request.

5 Implementation of policy

This Policy shall be deemed effective on 7th December 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

6 Review

This policy on data subject requests will be reviewed bi-annually, or when the Information Commissioner's Office (ICO) issues revised guidance on this topic.

Procedure for managing data subject requests

Data subject request response team

Requests from data subjects can create significant work, especially in the case of subject access requests. Other types of requests, such as objections to processing have the potential to disrupt the normal operation of the School

Failing to meet the requirements of a data subject request can result in enforcement action by Information Commissioner's Office and it is arguable that for the School the reputational damage is a greater risk than any potential fines.

This being the case, the delivery of data subject's requests needs to be managed by staff who are able to collect appropriate data or take the actions requested by the data subject without administrative delay.

The School has a Data Protection Team. This team comprises a permanent core team, supplemented by other members depending on the nature of the request being managed.

This Data Protection Team also includes

The Data Protection Officer

And include staff from:

- Information Technology
- Finance
- Quality
- Include others as appropriate

This teams need to reflect representation of the major functions within The School (Senior Leadership, Curriculum, Administration and IT).

Procedure overview

The procedure for managing data subject requests needs to be implemented in detail by the Data Protection Team across the School. These procedures need to take account of the following stages and requirements. The actions described in this section are by no mean exhaustive. The Data Protection Team may establish further detailed procedures and work instructions. Where this happens, they will be referred to in the main body of this policy.

I. Receiving a data subject request

II. Clarifying a request

III. Verifying the identity of the requestor

IV. Validating the request

V. Fulfilling the request

VI. Communications with the requestor

Receiving a data subject request

Unlike the 1998 Data Protection Act, there are no restrictions on how a person can register a request in respect of personal data belonging to them or a third party. Any member of staff of the School could be approached to commence a request.

It is, therefore, essential that all staff are made aware that they may receive the initiation of a request. This can come through any communications channel that the School provides, and this does include a verbal request made to a member of staff.

For the avoidance of doubt these channels include any social media accounts managed by the School, web-based enquiry forms and any voicemail systems in operation. Where email messages are distributed from accounts that are unmonitored, they must clearly state that no action will be taken on any messages sent to that address.

The School can choose to make a specific communications route available for making data protection requests or raising questions and complaints.

The School encourages the use of **DPA@hccs.info** for making data subject requests, although it recognises the right of individuals to make requests through any available route.

The School may choose to devote an area of the website to register requests. The School cannot refuse to deal with a request if it does not use the preferred route, nor require the data subject to resubmit the request.

The complexity and potential issues of responding to a data subject request means that it is not appropriate for staff outside of the Data Protection Team to respond. The primary responsibility of staff is to ensure that any request is passed on to the Data Protection Team. In the case of an enquiry being made in person, arrangements

should be made for the person to speak with a member of the data protection team, whether face to face or remotely

The School will set up appropriate routes for staff to notify the Data Protection Team.

This will include both telephone and email routes and provide details for contact outside of normal working hours or outside of term time.

To notify a data subject request in person please speak, in the first instance to Megan Ainsworth in the HR Team

It is important to recognise that the delivery time for a response to a subject access request is a maximum of one calendar month. This delivery window does not take account of the academic calendar. For example, a request can be received outside of term time and it is still expected to be delivered in the standard timescale.

The School has put measures in place to ensure that these communications routes are monitored outside of term time.

All incoming requests should be logged in a way that is available for the DPO to review

Clarify the request

It is possible that this stage is not necessary if the data subject has been very specific in their request. In most cases there is additional information required to ensure that the School has an accurate description of the action required.

This is most commonly seen with subject access requests where the lack of specificity by the data subject results in the entire personal data set relating to the individual being required. This can include records from IT Security equipment and entry management systems.

Especially where the potential dataset is very large, then a member of the data protection team may ask the requestor if they have any information that would enable the scope of the request to be reduced.

In the event that the relationship between the School and the data subject is very poor, this communication may be passed over to the data protection officer, whose role includes acting as an advocate for the data subject.

Although the School may ask the data subject to provide additional information to narrow the scope of the request, the data subject is under no obligation to do so. This may affect decisions about the validity of the request at a later stage in the procedure.

Verification of identity

If the School should respond to a data subject request, assuming that the person making the request is who they claim to be, and that results in some form of unauthorised disclosure or action, a breach has occurred that the Information Commissioner's would view as having been avoidable.

The GDPR (Recital 64) requires the data controller to use all reasonable efforts to verify the identity of the person making the request. This is particularly the case when the initial request is not received in person. The means of identification should also account for the existing relationship between the School and the data subject. In the case of a current student or member of staff then it is easy to establish their identity in person and through the use of School provided communications otherwise.

For other data subjects the School will go through a standard form of identity verification using photo identification and proof of address. In the case that the data subject cannot attend in person to present the documents, copies can be sent to the School and a videoconference can be used to check the person against the documents provided.

If this method cannot be used, the data protection officer should be consulted to look at alternatives.

If suitable verification is not possible then the request will not progress further.

Given the cohort at the School, special attention must be paid to any requests coming from parents of students for information about the student. Unless there is a question of the student not having the capacity to understand

the consequences of the request for personal data, or some other data subject request, it is expected that the request should be referred to the data subject directly.

Alternatively, the data subject can provide permission for the third party to complete the request. The same level of checking should be applied to the permission provided by the requestor and without suitable evidence the request cannot move forward.

For the avoidance of doubt, third parties such as Solicitors, Local Authorities and the Police Service cannot make a subject access request on behalf of a third party without appropriate consent. As an example, a letter from a solicitor saying that they are acting on behalf of an individual would not be sufficient without additional evidence.

There is no requirement to retain the evidence of identity gathered at this stage of the process, but the work done to establish identity should be recorded in the log of the request.

Validate the request

This stage is quite short. The requestor has been verified as an individual who is authorised to make a request. However, it is not the case that all data subject requests are available for all personal data. The key driver of the difference in rights available to a data subject is the legal basis of processing.

If there is uncertainty about the applicability of any particular right to particular items of personal data, the DPO should be consulted. However, it is the case that the right of access and the right to rectification apply irrespective of the legal basis of processing.

The fact that the majority of the personal data processed by the School is processed on the basis of performing a task in the public interest, significantly limits the rights available to the data subject.

The decision about validity and any associated communications should be recorded in the log of the request.

Fulfilling the request

Depending upon the nature of the data subject request this stage may be very short or extensive. Where the request is, for example the correction of an inaccurate item of personal data, this request should be met as soon as possible and requires limited effort. For the remainder of this section we will discuss the fulfilment of a subject access request which represents the greatest potential work.

The request will specify the data that is required to be collected. Details of locating that data can be drawn from the Record of Processing Activities. Data may be collected on paper and electronically. Electronic collection usually means getting an extract from a system containing the relevant information.

There are complex rules about the data that can be released and once the basic data has been collected these rules need to be considered. It is not possible to detail out all the potential exemptions to release and the exemptions to the exemptions.

In addition, any references to third parties should be redacted from the collected data before it can be released. Accidentally releasing information about third parties by failing to redact the response to a subject access request is generally considered a serious breach.

In some cases, where the task of redaction is unfeasible (most often with CCTV footage) a decision may be made that the information cannot be released even though it represents personal data of that data subject.

In some cases, other policies will override the data protection policy in respect of releasing information. This is especially the case with safeguarding information.

Where data is redacted or withheld, a record should be added to the log of the request.

Communications with the requester

Once the request has been fulfilled, for example a rectification has been done, or the response to a subject access request has been assembled, there is a requirement to communicate the response to the requestor.

In addition to the confirmation of the completion of the request the data subject or requestor should also be sent a copy of the privacy notice that is appropriate to them. This will meet the requirements to provide information about the way that personal data is processed.

Where the request was for subject access the results must be delivered to the requestor. For electronic responses a secure download, addressed to a validated email account is the preferred method.

On no account should the results be sent by email, a public sharing site, such as Dropbox, or on a removable drive.

Where the response is provided on paper, then ideally the individual should come in person to pick up the response and sign a receipt to confirm they have received the information. If this is not possible then the results should be sent by recorded delivery to a verified postal address, or if appropriate the results can be hand delivered, double enveloped.

In the case that the request cannot be met in the stipulated calendar month, a communication must be sent to the data subject setting out the reasons for the delay and the expected timescale for the completion of the request, this communication should be sent by the data protection officer.

Appendix 3: Data breach policy

1. Data breach team

Data breaches have 72 hours in total (from the point of detection) to be investigated, mitigated and assessed with respect to the need for notification to the Information Commissioner's Office (ICO). It should be noted that this is 72 elapsed hours including weekends and holidays.

Potential or actual data breaches pose the greatest threat in terms of financial penalty to the School and to its wider reputation. It is arguable that for the School the reputational damage is a greater risk than any potential fines.

This being the case, the management of personal data breaches needs to be managed by senior staff who are able, without restriction, to bring about immediate mitigation of a potential or actual breach.

The School has a Data Breach Team. This team comprises a permanent core team, supplemented by other members depending on the nature of the breach being managed.

This Data Breach Team will also include

The Data Protection Officer

And include staff from:

- Information Technology
- Finance
- Quality
- Include others as appropriate

The teams need to reflect representation of the major functions within The School (Senior Leadership, Curriculum, Administration and IT). The Data Protection Officer will need to be immediately informed and advise on actions to be taken on any potential or actual data breach.

2. Procedure overview

The procedure for managing personal data breaches needs to be implemented in detail by the Data Breach Team across the School. These procedures need to take account of the following stages and requirements. The actions described in this section are by no means exhaustive. The Data Breach Team may establish further detailed procedures and work instructions. Where this happens, they will be referred to in the main body of this policy.

I. Discovery of a personal data breach

II. Investigate the nature of the breach

III. Action to contain the breach

IV. Assess the level of notification required

V. Notify appropriate parties

VI. Identify actions to minimise the reoccurrence of the breach

3. Discovery of a personal data breach

This section covers both the initial recognition that a breach has occurred and the notification to the Data Breach Team to enable action to be taken.

Any member of staff at the School may identify that a breach has potentially occurred. They may also receive a report from a student or any other stakeholder that a potential breach has occurred. Section 9 of this document

lists some circumstances that upon discovery point to a likely data breach. It is essential to recognise that these are for guidance and illustration only. If in doubt, inform the Data Breach Team.

Reporting a breach makes a positive contribution to the School managing its' data protection responsibilities.

Although not all personal data breaches are reported to the Information Commissioner's Office, each incident should be treated as though it might be until the evidence shows otherwise.

It is, therefore, essential that when a potential breach is discovered that it is reported to the Data Breach Team as soon as possible.

The School has provided the email address DPA@hccs.info for communications about data protections issues

This will include both telephone and email routes and provide details for contact outside of normal working hours or outside of term time.

To notify a personal data breach in person please speak, in the first instance to the GDPR Lead.

The School has put measures in place to ensure that these communications routes are monitored outside of term time.

As mentioned in Section 1, in the case of a personal data breach that must be reported to the ICO, there is a 72-hour window. It should be noted that at the point any member of staff becomes aware of a potential breach this is the start of the 72-hour window, not when the Data Breach Team or the DPO is informed.

For example, if a member of staff discovers that their car has been broken into on Friday evening and a laptop is stolen – this is the discovery of the breach not when it is reported to the School after the weekend.

Members of staff are not expected to independently investigate potential breaches before bringing them to the attention of the Data Breach Team as this will reduce the time available for the Data Breach Time to manage the issue.

Information required when reporting a breach:

From the initial report, it is essential to establish a chronology for the breach. This will later include information about actions taken and impact assessments. At this first stage the person reporting the breach needs to provide:

i. The time and date that the suspected breach was detected

ii. A description of the nature of the breach including classification (Confidentiality, Availability, Integrity)

iii. The data subjects, types of personal data and number of records affected

iv. How the individual identified the potential breach

v. Details of any individuals they have discussed the potential breach with

If there are emails or other notes, call records or any other materials associated with the discovery of the breach, these should be provided although it is recognised that there may be a delay in assembling all the material.

It should be noted that depending on the exact circumstances, the person who has identified the potential breach may have minimal information.

4. Investigate the nature of the breach

The core focus at this stage is to have enough information to determine if notification to the ICO will be required. The report from the individual who discovers the breach may not have sufficient detail to make the decision. To make this decision the essential information is:

- The type and numbers of data subjects affected
- The types of personal data compromised and the number of records
- Initial assessment of the cause of the breach
- The possible consequences of the breach

- Any factors that mitigate the risk from the breached data

The leader of the Data Breach Team will assign appropriate members of the team to undertake the investigation. This may require additional assistance from the person who discovered the breach.

If possible, information gathered during the investigation should be supported by records, emails, or by reference to other school sources.

At any point in the investigation the Data Breach Team may decide they have enough information to make the assessment of notification. This does not mean that the investigation is complete, but the decision will determine the timescale for the completion of other activities.

Any documents, notes of meeting, or calls and emails should be recorded on the chronology.

5. Take containment action

Containment means taking action that mitigates the potential consequences of the breach. Providing a breach has been reported quickly, significant mitigation may be possible. In some cases, especially with confidentiality breaches, the time gap between the initial breach and its discovery leaves little room for containment.

Before undertaking any action, an assessment must be made to ensure that it doesn't compound the breach – for example by disclosing personal data to additional unauthorised recipients.

If, at this point, criminal activity is suspected (even tangentially, such as the theft of a car containing personal data), the police should be informed, and the crime number should be recorded. If there is strong evidence that a member of the school community has deliberately breached information, then appropriate disciplinary action needs to be initiated.

Even if the actual breach event happened some time before discovery, the questions about whether actions can be taken to mitigate the further spread of breached information should be considered. It can of course be far more difficult to achieve in these circumstances.

Whatever decisions and actions are taken, should be recorded in the breach log chronology.

6. Assess the level of notification required

This is a decision that must involve the leader of the Data Breach Team. The guidance of the Data Protection Officer should be sought, although the Data Breach Team is free to make decisions based on more than the data protection issues.

There are no simple threshold numbers that can be used. Highly confidential information about a small number of people could have very significant impacts on them or other people, while relatively benign data about many people may have little risk to their rights and freedoms.

Each case must be decided upon its specific circumstances and ideally the team should be unanimous. The team should be aware that the Data Protection Officer, in fulfilling their role, may decide that the ICO must be alerted to even though the Data Breach Team have decided not to report an incident

The rationale for the decision about reporting should be recorded and kept with other details of the breach. If a judgement Is made that the ICO must be notified, then it's likely that further investigation will be required before the report can be completed. This means that this decision about notification really needs to come well before the 72-hour window closes.

7. Notification of the breach (where required)

This task, unless there are exceptional circumstances, will be carried out by the Data Protection Officer. Part of the role is to be the interface between the data controller and the regulator. The critical requirement is for the investigation to have been completed and any potential action to contain the breach needs to be in progress or planned.

Members of the Data Breach Team will need to be available to answer any questions that the ICO may have and to take actions that are recommended.

If notification to the ICO is not required, then the information about the breach in the chronology will be completed and the entry in the breach log will be closed. The same basic information that would go into the ICO notification should go into the local breach log. For local logging the 72-hour timescale is not enforced.

8. Repair the causes of the breach

For organisations to be fully GDPR compliant they need to be able to demonstrate that they have engineered data protection by default and by design into their operations. One element of that is to look for continuous improvement in the data protection regime.

Any incident that has been recorded on the breach log should be subject to review. The review team would certainly include members of the Data Breach Team but may also include other senior colleagues.

Reviews of specific incidents should be recorded such that they can be filed with the records of the incident.

It may be that the review of an individual case identifies weaknesses in the data protection regime and the team should certainly go on to consider how these weaknesses can be addressed. The review team should also bear in mind that sometimes there is a pattern of incidents (for example a skew in the distribution of days of the week that incidents occur). These patterns may reveal something systemic in the organisation that needs to be addressed.

If there have been significant breaches, then the review team can consider whether a Data Protection Impact Assessment (DPIA) would be useful to identify specific weaknesses in the processing of personal data in the area of the breach.

Minutes and actions of the review team meeting should be kept and retained for the current year and two years afterwards.

9. Possible indications of personal data breaches (not exhaustive)

The items described in this section form a very small subset of the signs that a breach has occurred. It is essential to remember that there is no requirement to know that the rights and freedoms of individuals have been infringed to recognise that a breach has occurred. It is enough that the infringement could happen.

Consider the three types of personal data breaches – confidentiality, availability and integrity. Many real-world situations combine categories.

For example: A missing paper file of SEND information means that an expected assessment can't be carried out. When the file is retrieved by the member of staff who took it home, it is discovered that some of the information has been out of date for 18 months. This is the combination of an availability and an integrity breach.

10. <u>Confidentiality Breaches</u>

Here we are concerned about information falling into the hands of people unauthorised to have it. Obvious cases would be.

- Loss or theft of a computer, tablet or phone containing, or with access to, personal data
- Loss or theft of a personal bag containing paper records of personal data
- An individual having access to, or a copy of, personal data not required for their role (note here that if person has a role requiring them to produce and manage personal data even though then are not involved the process that uses the data this is not a breach)
- Sending an email to the wrong location
- Disclosing the identity of recipients of an email when those recipients might otherwise reasonably expect confidentiality.

● Passing on information about a data subject from an individual who is entitled to know to one who is not entitled

In some cases, it would be relatively easy to identify that the breach had occurred, but in others the initial indications of the breach may be quite diffuse. For example, staff may discover a case of intimidation or bullying and then recognise that it has been based on personal data which might have been obtained in an inappropriate fashion.

In extreme cases the first indication of a breach is the lodging of a complaint with the School or the appearance of stories in the traditional media or in social media spaces.

11. Availability Breaches

An availability breach is probably the easiest to spot because information is not available when it's required.

Possible causes might be:

- A failure of a system like the MIS, HR Database or Visitor Management
- A file not being returned to its storage location
- A file being shredded before the end of its retention period
- Records being erased before their retention period
- Theft, fire or vandalism

There are thresholds to consider in the case of an availability breach. If a system is down for a short period of time, or missing for a short period, then this would almost certainly not meet the threshold. The question is whether the lack of availability could have an impact on the rights and freedoms of the data subjects that the information is related to.

Integrity Breaches

Integrity breaches occur when personal data is inaccurate. There are two major ways that this occurs

- Data is captured inaccurately
- The data becomes out of date

The breach only appears at the time the data is being retrieved or used and the potential impact of the breach can be highly variable.