Policies

Data Protection Policy & Procedure

Next review date: June 2027

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

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 the 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 Complaints

32.1 Purpose and Scope

This procedure outlines how HCCS handles complaints related to the processing of personal data, in accordance with UK data protection law. It applies to all individuals who believe we have infringed their rights under the UK General Data Protection Regulation (UK GDPR) and/or the Data Protection Act 2018 (as amended).

32.2 How to Lodge a Complaint

If you have concerns about how we collect, use, store, or share your personal data, you can lodge a complaint in any of the following ways:

- Online Form: https://www.hccs1978.co.uk/concerns-and-complaints
- Email: DPA@hccs.info
- Post: Holmes Chapel Comprehensive School, Selkirk Drive, Holmes Chapel, Cheshire, CW4 7DX

You do not need to use a specific format, but please include:

- Your full name and contact details
- A clear description of your complaint
- The data or processing activity involved (if known)
- Any evidence or relevant correspondence
- The outcome or remedy you are seeking (if applicable)

32.3 What Happens Next?

Acknowledgement - We will acknowledge your complaint within 30 calendar days of receipt.

Investigation -We will review your complaint and may contact you for further information. The investigation will be handled by our Data Protection Officer or a designated privacy lead.

Response - We aim to respond without undue delay, and in most cases, within one calendar month of receipt. If the matter is complex, we may extend this by up to two further months—but we will inform you and explain why.

32.4 Escalation: Your Rights

If you are not satisfied with our response, or you believe we have not handled your complaint appropriately, you have the right to escalate the matter to the Information Commissioner's Office (ICO):

- Website: https://ico.org.uk/make-a-complaint/
- Phone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

However, under the Data (Use and Access) Act 2025, the ICO may require that you first submit your complaint to us before they investigate

32.5 Record Keeping

All complaints and responses will be logged and retained for 6 years, in accordance with our privacy and compliance obligations.

32.6 Contact Us

If you have questions about this procedure or your data protection rights, please contact:

Data Protection Administrator
Email: dpa@hccs.info
Address: Holmes Chapel Comprehensive School, Selkirk Drive, Holmes Chapel, Cheshire, CW4 7DX

33 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 2027

Appendix 1: Data retention and disposal policy

1.1 Application

This Policy sets out the measures adopted by HCCS 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

Contracts

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Contracts	**Contracts**	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years or end of contract + 12 years, whichever is the longer	Limitation Act 1980	SECURE DISPOSAL	
	Contracts	All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years or end of contract + 6 years whichever is the longer	Limitation Act 1981	SECURE DISPOSAL	
	Contracts	Records relating to the management of contracts with external providers	No	End of contract + 6 years or date of last payment on contract + 6 years whichever is the longer		SECURE DISPOSAL	
	Contracts	Records relating to the monitoring of contracts	No	End of the contract or until the final payment has been made whichever is the longer		SECURE DISPOSAL	
	Contracts	All records relating to the maintenance of the school carried out by contractors	No	Current year + 6 years. This may vary on the type of maintenance. Records relating to rewiring, major alterations etc must be retained in the health and safety file whilst the building belongs to the school and must be passed onto any new owners if the building is leased or sold.		SECURE DISPOSAL	

	Contracts	All records relating to the maintenance of the school carried out by school employees, including maintenance log books	No	Life of equipment + 6 years. Alterations to wiring and major modifications must be entered in to the health and safety file		SECURE DISPOSAL	
	Contracts	Records relating to the management of software licences	No	Date licence expires + 6 years		SECURE DISPOSAL	

Education Management

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Education Management	**Management Information**	Published Admission Number (PAN) reports	Yes	Current year + 6 years		SECURE DISPOSAL	
	Management Information	Curriculum returns	No	Current year + 3 years		SECURE DISPOSAL	
	Management Information	Self-evaluation forms	Yes	Current year + 6 years		SECURE DISPOSAL	
	Management Information	Self Evaluation Forms - External moderation	Yes	Until superseded		SECURE DISPOSAL	
	Management Information	Self Evaluation Forms - Internal moderation	Yes	Academic year plus one academic year		SECURE DISPOSAL	
	Management Information	Value added and contextual data	Yes	Current year + 6 years		SECURE DISPOSAL	

	Policies and Frameworks	Complaints Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Policies and Frameworks	Data Protection Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Policies and Frameworks	Freedom of Information Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Policies and Frameworks	Information Security Breach Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	

	Policies and Frameworks	Special Educational Needs Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Policies and Frameworks	Equality Information and Objectives (public sector equality duty). Statement for publication	No	Life of statement or date statement superseded + 3 years		SECURE DISPOSAL	
	Policies and Frameworks	Risk and Control Framework	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Policies and Frameworks	Rules and Bylaws	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	
	Strategy	Strategic Review	No	Life of the review or until review superseded + 3 years. If major changes are made to the review then an archive copy of previous review		SECURE DISPOSAL	

				should be retained			
	Strategy	Strategic Plan [also known as School Development Plans]	No	Life of the review or until review superseded + 3 years. If major changes are made to the review then an archive copy of previous review should be retained		SECURE DISPOSAL	
	Strategy	Accessibility Plan	No	Life of the review or until review superseded + 3 years. If major changes are made to the review then an archive copy of previous review should be retained	Equality Act 2010	SECURE DISPOSAL	

Examinations

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Examinations	**Examinations**	SATs records Examination papers	Yes	The examination papers should be kept until any appeals/validation process is complete		SECURE DISPOSAL	

	Examinations	SATs records Results	Yes	The SATS results should be recorded on the pupils 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	
	Examinations	Examination Results Pupil Copies: Public	Yes	This information should be added to the pupil file		Schools should follow the instructions of the Examination Board about disposing of uncollected certificates	
	Examinations	Examination results pupil copies: Internal	Yes	This information should be added to the pupil file			
	Examinations	Examination results (schools copy)	Yes	Current year + 6 years		SECURE DISPOSAL	
	Examinations	Management of examination registrations	Yes	The examination board will usually mandate how long these records need to be retained			

Extra Curriculum and Miscellaneous Activities

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Extra Curriculum and Miscellaneous Activities	**Extra Curriculum and Miscellaneous Activities**	Records created by schools in order to obtain approval to run an educational visit outside the classroom - Primary schools	No	Date of Visit + 15 years	Limitation Act 1980	SECURE DISPOSAL	
	Extra Curriculum and Miscellaneous Activities	Records created by schools in order to obtain approval to run an educational visit outside the classroom - Secondary schools	No	Date of visit + 15 years	Limitation Act 1980	SECURE DISPOSAL	
	Extra Curriculum and Miscellaneous Activities	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 date of birth + 25 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		SECURE DISPOSAL	One-off or blanket consent: The Department for Education (DfE) has prepared a one-off consent form to be signed by the parent on enrolment of their child in a school. This form is intended to cover all types of visits and activities where parental consent is required. The form is available on the DfE website for establishments to adopt and adapt, as appropriate, at https://www.gov.uk/government/publications/consent-for-school-trips-and-other-off-site-activities. A similar form could be used for other establishments, such as Early Years Foundation Stage (EYFS) providers and youth groups, or at the start of programmes for young people.

	Extra Curriculum and Miscellaneous Activities	Parental permission slips for school trips where there has been a major incident	Yes	Date of birth of the pupil involved in the incident + 25 years or 15 years after the incident whichever is the longer. 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	Limitation Act 1980	SECURE DISPOSAL	
	Extra Curriculum and Miscellaneous Activities	Records relating to residential trips	Yes	Date of birth of youngest pupil involved + 25 years or if there is a major incident then date of incident + 15 years whichever is the longer	Limitation Act 1980	SECURE DISPOSAL	

Finance

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Finance	**Funding**	Funding Agreement with Secretary of State and supplemental funding agreements [Where there is multi-Academy governance.]	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	

	Funding	Funding Agreement Termination of the funding agreement	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	Either party may give not less than 7 financial years written notice to terminate the Agreement, such notice to expire on 31 August. Or, where the Academy has significant financial issues or is insolvent, the Agreement can be terminated by the Secretary of State to take effect on the date of the notice.
	Funding	Funding Records Capital Grant	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	
	Funding	Funding Records Earmarked Annual Grant (EAG)	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	
	Funding	Funding Records General Annual Grant (GAG)	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	
	Funding	Per pupil funding records	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	
	Funding	Funding records	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	Funding agreement which says that the Academy can receive donations and can only charge where the law allows maintained schools to charge [see Charging and Remission Policy].
	Funding	Gift Aid and Tax Relief	Yes	Date of last payment of funding + 6 years		SECURE DISPOSAL	
	Funding	Exclusions agreement	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	The Academy can enter into an arrangement with a Local Authority (LA), so that payment will flow between the Academy and the LA, in the same way as it would do were the Academy a maintained school.
	Funding	Records relating to loans	No	Date of last payment on loan + 6 years if the loan is under 10,000 or date of last payment on loan + 12 years if the loan is over 10,000		SECURE DISPOSAL	
	Funding	Management of Endowment Funds	No	Life of the fund + 6 years		SECURE DISPOSAL	

	Funding	Investment policies	No	Life of the investment + 6 years		SECURE DISPOSAL	
	Funding	Pupil Premium Fund records	Yes	Date pupil leaves the provision + 6 years		SECURE DISPOSAL	
	Funding	Student Grant applications	Yes	Current year + 3 years		SECURE DISPOSAL	
	Operational	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years		SECURE DISPOSAL	
	Operational	Records relating to the collection and banking of monies	No	Current financial year + 6 years		SECURE DISPOSAL	
	Operational	Records relating to the identification and collection of debt	Yes	Payment or write off of debt + 6 years		SECURE DISPOSAL	

	Risk Management and Insurance	Employers Liability Insurance Certificate	No	Year of issue + 40 years. Pass to the Local Authority if the school closes	EXPLANATORY NOTE (This note is not part of the Regulations) These Regulations amend the Employers' Liability (Compulsory Insurance) Regulations 1998 (the 1998 Regulations). Regulation 2(1) omits paragraphs (4) and (5) from regulation 4 of the 1998 Regulations. Paragraph (4) required an employer to retain a copy of its employer liability insurance certificate for 40 years. Paragraph (5) was a consequential provision to paragraph (4), providing for the retention of certificates, and is therefore also being omitted. Paragraph (3) substitutes paragraphs (1) and (2) of regulation 5 of the 1998 Regulations. Under the new provisions, the	SECURE DISPOSAL	

					requirements for the display of the certificate will be satisfied if the certificate is made available in electronic form and is reasonably accessible to the relevant employees. Paragraph (4) makes a consequential amendment to regulation 6(b) of the 1998 Regulations.		

	Risk Management and Insurance	Insurance policies	No	Date the policy expires + 6 years except Public Liability insurance - day of issue + 40 years	EXPLANATORY NOTE (This note is not part of the Regulations) These Regulations amend the Employers' Liability (Compulsory Insurance) Regulations 1998 (the 1998 Regulations). Regulation 2(1) omits paragraphs (4) and (5) from regulation 4 of the 1998 Regulations. Paragraph (4) required an employer to retain a copy of its employer liability insurance certificate for 40 years. Paragraph (5) was a consequential provision to paragraph (4), providing for the retention of certificates, and is therefore also being omitted. Paragraph (3) substitutes paragraphs (1) and (2) of regulation 5 of the 1998 Regulations. Under the new provisions, the	SECURE DISPOSAL	

					requirements for the display of the certificate will be satisfied if the certificate is made available in electronic form and is reasonably accessible to the relevant employees. Paragraph (4) makes a consequential amendment to regulation 6(b) of the 1998 Regulations.		
	Risk Management and Insurance	Records relating to the settlement of insurance claims	Yes	Date claim settled + 6 years		SECURE DISPOSAL	
	Risk Management and Insurance	Burglary, theft and vandalism report forms		Current year + 6 years		SECURE DISPOSAL	
	Risk Management and Insurance	Audit Committee and appointment of responsible officers	No	As long as necessary		SECURE DISPOSAL	Life of Academy. Under the Companies Act members can have their details removed after a certain time. Details should be removed on request.
	School Fund	School Fund Ledger	Yes [ledger may contain names of people in receipt of grants]	Current financial year + 6 years		SECURE DISPOSAL	
	School Fund	Whole of government accounts returns	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Fund	School Fund Journey books	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Fund	School Fund Invoices	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Fund	School Fund Receipts	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Fund	School Fund Bank statements	No	Current financial year + 6 years		SECURE DISPOSAL	

	School Fund	School Fund Cheque books	No	Current financial year + 1 year		SECURE DISPOSAL	
	School Fund	School Fund Paying in books	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Meals	Free school meals registers	Yes	Current financial year + 3 years		SECURE DISPOSAL	
	School Meals	School meals summary sheets	No	Current financial year + 6 years		SECURE DISPOSAL	
	School Meals	School meals registers	Yes	Current financial year + 3 years		SECURE DISPOSAL	
	Strategic Finance	Annual accounts	No	Current financial year + 6 years		SECURE DISPOSAL	
	Strategic Finance	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	
	Strategic Finance	Statement of financial activities for the year	No	Current financial year + 6 years		SECURE DISPOSAL	
	Strategic Finance	Financial Planning	No	Current financial year + 6 years		SECURE DISPOSAL	
	Strategic Finance	Value for money statement	No	Current financial year + 6 years		SECURE DISPOSAL	
	Strategic Finance	Borrowing powers	No	Until superseded + 6 years		SECURE DISPOSAL	
	Strategic Finance	Charging and remissions policy	No	Date policy superseded + 3 years		SECURE DISPOSAL	
	Strategic Finance	Independent Auditors report on regularity	No	Financial year report relates to + 6 years		SECURE DISPOSAL	
	Strategic Finance	Independent Auditors report on financial statements	Yes	Financial year report relates to + 6 years		SECURE DISPOSAL	
	Strategic Finance	Records relating to the management of VAT	No	Current financial year + 6 years		SECURE DISPOSAL	

Governing Bodies

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Governing Bodies	**Activities**	Records relating to Governor Monitoring Visits	Yes	Date of the visit + 3 years		SECURE DISPOSAL	
	Governance	Constitution	No	Date constitution superseded + 10 years. It may be appropriate to retain one copy of each constitution for archival purposes	Companies Act 2006 section 355	SECURE DISPOSAL	Companies Act 2006 Section 355: This section refers to Records of Resolutions and meetings etc. it does not mention Constitutions. Resolutions and minutes under this section to be retained for at least 10 years from date of meeting or decision as appropriate (Section 355 (2))
	Governance	Articles of Association	No	Life of the Academy		SECURE DISPOSAL	
	Governance	Memorandum of Association	No	This can be disposed of once the Academy has been incorporated		SECURE DISPOSAL	
	Governance	Memorandum of Understanding of Shared Governance among Schools	No	Life of Memorandum of Understanding + 6 years		SECURE DISPOSAL	
	Governance	Governance Statement	No	Life of governance statement + 6 years. One copy of each iteration may need to be retained for archive purposes		SECURE DISPOSAL	
	Governance	Written Scheme of Delegation	Yes	Life of Written Scheme of Delegation + 10 years	Companies Act 2006 section 355	SECURE DISPOSAL	
	Governance	Special Resolutions to amend the Constitution	No	Date constitution superseded + 10 years. It may be appropriate to retain one copy of each constitution for archival purposes	Companies Act 2006 section 355	SECURE DISPOSAL	Companies Act 2006 section 355 Section 355: This section refers to. Records of Resolutions and meetings etc. it does not mention. Constitutions. Resolutions and minutes under this section to be retained for at least 10 years from date of meeting or decision as appropriate (Section 355 (2))
	Governance	Annual Report and Accounts	No	Date of report + 10 years	Companies Act 2006 section	SECURE DISPOSAL	

					356		
	Governance	Annual Report Trustees Report	No	Date of report + 10 years	Companies Act 2006 section 357	SECURE DISPOSAL	
	Governance	Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years		SECURE DISPOSAL	
	Governance	Annual Return	No	Date of report + 10 years	Companies Act 2006 section 357	SECURE DISPOSAL	
	Governance	Instruments of Government	No	For the life of the school		Consult local archives before disposal	
	Governance	Register of Directors	Yes	Date Director resigns + 10 years	Companies Act 2006	SECURE DISPOSAL	Companies Act Section121 Removal of entries relating to former members. An entry relating to a former member of the company may be removed from the register after the expiration of ten years from the date on which he ceased to be a member
	Governance	Scheme of Delegation and Terms of Reference for Committees	No	Until superseded or whilst relevant [Schools may wish to retain these records for reference purposes in case decisions need to be justified]		These could be offered to the archives if appropriate	
	Governance	Trusts and Endowments managed by the Governing Body	Yes	Life of the Trust or Endowment + 6 years		SECURE DISPOSAL	

	Governance	Records relating to complaints dealt with by the Governing BodyAnnual Report and Accounts	Yes	Date complaint resolved + 3 years then review. If the complaint relates to negligence or safeguarding then date the complaint resolved + 15 years. If the complaint relates to child sexual abuse then the complaint resolved + 75 years (this retention period will be reviewed once the government and the ICO have issued guidance about the implementation of the IICSA recommendations)		SECURE DISPOSAL	
	Governance	All records relating to the conversion of schools to Academy status	No	For the life of the organisation	Companies Act 2006 section 355	Consult local archives before disposal	
	Governance	Policy documents created and administered by the Governing Body	No	Until superseded. The School should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the government and ICO have published guidance about the implementation of the recommendations made in the IICSA report		SECURE DISPOSAL	

	Governors, Directors and Trustees	Appointment of Trustees and Governors and Directors	Yes	Life of appointment + 6 years	Companies Act 2006 section 355	SECURE DISPOSAL	
	Governors, Directors and Trustees	Records relating to the election of parent and staff governors not appointed by the governors	Yes	Date of election + 6 months		SECURE DISPOSAL	
	Governors, Directors and Trustees	Records relating to the appointment of co-opted governors	Yes	Provided that the decision has been recorded in the minutes the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office except where there have been allegations concerning children. In this case retain for 25 years.		SECURE DISPOSAL	
	Governors, Directors and Trustees	Records relating to the terms of office of serving governors including evidence of appointment	Yes	Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years.			
	Governors, Directors and Trustees	Records relating to Governor Declaration against disqualification criteria	Yes	Date appointment ceases plus 6 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Governors Code of Conduct	No	This is expected to be a dynamic document, one copy of each version should be kept for the life of		SECURE DISPOSAL	

				the organisation			
	Governors, Directors and Trustees	Records relating to DBS checks carried out on clerk and members of the governing body	Yes	Date of DBS check + 6 months (but need to retain a record of the date of the DBS check if you are renewing every 3-5 years depending on policy)		SECURE DISPOSAL	
	Governors, Directors and Trustees	Governor personnel files	Yes	Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Records relating to the induction programme for new governors	Yes	Date appointment ceases plus 6 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Records relating to the training required and received by Governors	Yes	Date Governor steps down + 6 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Appointment and removal of Members	No	Life of appointment + 6 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Register of members		Date Member resigns + 10 years	Companies Act 2006	SECURE DISPOSAL	
	Governors, Directors and Trustees	Statement of Trustees Responsibilities	No	Life of statement + 6 years		SECURE DISPOSAL	
	Governors, Directors and Trustees	Register of Trustees interests	Yes	Date Trustee resigns + 10 years	Companies Act 2006	SECURE DISPOSAL	

	Governors, Directors and Trustees	Declaration of Interests Statements [Governors] [this is not a statutory register]	Yes	Date Governor resigns + 10 years		SECURE DISPOSAL	
	Meetings	Board Meeting Minutes	Yes	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	
	Meetings	Board Decisions	Could be if the decisions refer to living individuals	Date of the meeting + a minimum of 10 years		OFFER TO ARCHIVES	
	Meetings	Board Meeting: Annual Schedule of Business	No	Current year		SECURE DISPOSAL	
	Meetings	Board Meeting: Procedures for conduct of meeting	No	Date procedures superseded + 6 years	Limitation Act 1980 (Section 2)	SECURE DISPOSAL	
	Meetings	Records relating to the management of General Members Meetings	No	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	
	Meetings	Minutes relating to any committees set up by the Board of Directors	Could be if the minutes refer to living individuals	Date of the meeting + a minimum of 10 years		OFFER TO ARCHIVES	
	Meetings	Records relating to the management of the Annual General Meeting	Could be if the minutes refer to living individuals	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	
	Meetings	Meetings Schedule	No	Current year		STANDARD DISPOSAL	

	Meetings	Agendas for Governing Body meetings	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	
	Meetings	Agendas Additional Copies	No	Date of meeting		STANDARD DISPOSAL	
	Meetings	Minutes of, and papers considered at, meetings of the Governing Body and its committees: Principal Set (signed)	May be data protection issues, if the meeting is dealing with confidential issues relating to staff	Date of meeting + 10 years		OFFER TO ARCHIVES	
	Meetings	Minutes of, and papers considered at, meetings of the Governing Body and its committees: Inspection Copies	Yes - May have names and personal issues unless redacted	Date of meeting + 10 years		SECURE DISPOSAL	
	Meetings	Reports presented to the Governing Body	Yes	Date of meeting the report was presented to + 10 years		SECURE DISPOSAL or retain with the signed set of minute	
	Meetings	Reports made to the Governors Meeting which are referred to in the minutes	Potential	Although generally kept for the life of the organisation, the Local Authority is only required to make these available for 10 years from the date of the meeting.	Companies Act 2006	Consult local archives before disposal	

	Meetings	Register of attendance at Full Governing Board meetings	Yes	Date of last meeting in the book + 6 years		SECURE DISPOSAL	
	Meetings	Papers relating to the management of the Annual Parents Meeting	Yes	Date of meeting + 6 years		SECURE DISPOSAL	

Health and Safety

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Health and Safety	**Health and Safety**	Health and Safety policy statements	No	Life of policy + 3 years		SECURE DISPOSAL	
	Health and Safety	Health and safety file to show current state of building including all alterations (wiring, plumbing, building works etc) and to be passed on in the case of change of ownership)	No	Pass to new owner on sale or transfer of building			
	Health and Safety	Fire precautions log books	No	Current year + 6 years		SECURE DISPOSAL	
	Health and Safety	Fire risk assessments	No unless containing Personal Emergency Evacuation plans	Life of the risk assessment + 3 years	Fire Service Order 2005	SECURE DISPOSAL	

	Health and Safety	Accident reporting: Adults	Yes	Date of last entry in the accident book + 3 years but if there is possibility of negligence allegation then date of incident + 15 years or date of settlement + 6 years	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	SECURE DISPOSAL	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below IRMSTK17.9 Do not keep completed entries in the book. They must be removed and kept in a locked location.
	Health and Safety	Records relating to accident/injury at work including incident reports	Yes	Date of incident plus 6 years unless the injury is serious - broken limb, more than 3 days in hospital etc then date of incident plus 15 years (Negligence)		SECURE DISPOSAL	
	Health and Safety	Accident reporting: Children	Yes	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below IRMSTK17.9 Do not keep completed entries in the book. They must be removed and kept in a locked location.	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	SECURE DISPOSAL	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below [see also the incident reporting form]

	Health and Safety	Control of Substances Hazardous to Health (COSHH)	No	COSHH sheets should be kept whilst the substance is in use + 6 years COSHH policy documents should be kept until the policy is superseded + 6 years		ECURE DISPOSAL	
	Health and Safety	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Yes	Date of incident + 3 years provided that all records relating to the incident are held on personnel file. See IRMSTK17.5 and IRMSTK17.7	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12(2)	SECURE DISPOSAL	For more information see: http://www.hse.gov.uk/RIDDOR/ https://www.hse.gov.uk/pubns/edis1.htm concerns schools
	Health and Safety	Health and Safety risk assessments	No	Life of risk assessment + 3 years		SECURE DISPOSAL	
	Health and Safety	Process of monitoring of areas where employees and persons have or are likely to have come into contact with asbestos	Yes	Last action + 40 years	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	SECURE DISPOSAL	

	Health and Safety	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation: Dose assessment and recording	No	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. To keep the records made and maintained or a copy of these records until the person to whom the record relates has or would have attained the age of 75 years but in any event for at least 30 years from when the record was made	The Ionising Radiations Regulation 2017	SECURE DISPOSAL	

Liaison with LEA-DFE

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Liaison with LEA-DFE	**Liaison with LEA-DFE**	OFSTED reports and papers	No	Life of the report then REVIEW		SECURE DISPOSAL	
	Liaison with LEA-DFE	Returns made to central government	No	Current year + 6 years		SECURE DISPOSAL	
	Liaison with LEA-DFE	School census returns	No	Current year + 5 years		SECURE DISPOSAL	
	Liaison with LEA-DFE	Circulars and other information sent from the Local Authority		Operational use		SECURE DISPOSAL	
	Liaison with LEA-DFE	Circulars and other information sent from central government	No	Operational use		SECURE DISPOSAL	

	Liaison with LEA-DFE	Attendance returns	Yes	Academic year + 1 year		SECURE DISPOSAL	
	Liaison with LEA-DFE	Secondary transfer sheets (Primary)	Yes	Academic year + 2 years		SECURE DISPOSAL	

Parent Teacher Association

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Parent Teacher Association	**Parent Teacher Association**	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Yes	Current year + 6 years then REVIEW		SECURE DISPOSAL	

Property

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Property	**Property**	Title deeds of properties belonging to the school	No	These should follow the property, unless the property has been registered with the Land Registry		Transfer to new owner	
	Property	Plans of property belonging to the school, including any alterations. This is also a health and safety requirement and includes rewiring diagrams and additional fire safety features	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		Pass to next owner	

	Property	Leases of property leased by or to the school	No	Expiry of lease + 6 years		SECURE DISPOSAL	
	Property	Business continuity and disaster recovery plans	Yes	These are dynamic documents which should be kept up to date		SECURE DISPOSAL OF OLD PLANS	
	Property	Records relating to the letting of school premises	No	Current financial year + 6 years		SECURE DISPOSAL	

Pupils and Students

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes

Pupils and Students	**Pupils and Students**	Pupils Educational Record required by The Education (Pupil Information) (England) Regulations 2005: Primary	Yes	Retain whilst the child remains at the primary school	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437	The file should follow the pupil when they leave 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 LA 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 school should discuss with the local authority about where the file should be stored for the remainder of its statutory retention	

	Pupils and Students	Pupils Educational Record required by The Education (Pupil Information) (England) Regulations 2005: Secondary	Yes	Date of birth of the pupil + 25 years	Limitation Act 1980 (Section 2)	SECURE DISPOSAL	Section 2: Time limit for actions founded on tort. An action founded on tort shall not be brought after the expiration of 6 years from the date on which the cause of action accrued
	Pupils and Students	Attendance registers	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	School attendance Guidance for maintained schools, academies, independent schools and local authorities [updated and re-published annually]	SECURE DISPOSAL	
	Pupils and Students	Correspondence relating to any absence (authorised or unauthorised)	Potential	Current academic year + 2 years	Education Act 1996 Section 7	SECURE DISPOSAL	

School Admissions

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
School Admissions	**School Admissions**	All records relating to the creation and implementation of the School Admissions Policy	No	Life of the policy + 7 years. 15(2) of the regulation refers to the 7 preceding years	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	

	School Admissions	Register of admissions	Yes	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made.	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities.	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	
	School Admissions	Admissions if the appeal is unsuccessful	Yes	Resolution of case + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	
	School Admissions	Admissions if the admission is successful	Yes	Date of admission + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	
	School Admissions	Admissions Secondary Schools Casual	Yes	Current academic year + 1 year		SECURE DISPOSAL	

	School Admissions	Proofs of address supplied by parents as part of the admissions process	Yes	Current academic year + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	
	School Admissions	Supplementary information form, including additional information such as religion and medical conditions: For successful admissions	Yes	This information should be added to the pupil file		As per pupil file	
	School Admissions	Supplementary information form, including additional information such as religion and medical conditions: For unsuccessful admissions.	Yes	Until appeals process completed		SECURE DISPOSAL	
	School Admissions	Records relating to the management of exclusions	Yes	Date of birth of the pupil involved + 25 years		SECURE DISPOSAL	

School Assets

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
School Assets	**School Assets**	Community School leases for land	No	Date lease expires + 6 years		SECURE DISPOSAL	

	School Assets	Commercial transfer arrangements	No	Date of transfer + 6 years		SECURE DISPOSAL	
	School Assets	Transfer of land to the Academy Trust	No	Life of land ownership then transfer to new owner		SECURE DISPOSAL	
	School Assets	Transfers of freehold land	No	Life of land ownership then transfer to new owner		SECURE DISPOSAL	
	School Assets	Records relating to the leasing of shared facilities, such as sports centres	No	End of lease + 6 years		SECURE DISPOSAL	
	School Assets	Land and building valuations	No	Date valuation superseded + 6 years		SECURE DISPOSAL	
	School Assets	Disposal of assets	No	Date asset disposed of + 6 years		SECURE DISPOSAL	
	School Assets	Burglary, theft and vandalism report forms	No	Date of insurance settlement + 6 years		SECURE DISPOSAL	
	School Assets	Inventories of furniture and equipment	No	Life of equipment + 6 years. Equipment will have write-down value over several years - the time depending on the type of equipment		SECURE DISPOSAL	

School Management

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes

School Management	**School Management**	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff	Date of last entry in the book + a minimum of 6 years then REVIEW		These could be of permanent historical value and should be offered to the County Archives Service, if appropriate	
	School Management	Visitor Management Systems (including electronic systems, visitors books and signing in sheets)	Yes	Academic Year + 1 year [Schools may decide to archive one copy]		SECURE DISPOSAL	
	School Management	School Privacy Notice which is sent to parents as part of GDPR compliance	No	Life of the privacy notice/until the privacy notice plus 6 years		SECURE DISPOSAL	
	School Management	Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)	Yes	Consents should be retained for as long as the consent is relied on.		SECURE DISPOSAL	

	School Management	Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current year + 1 year		STANDARD DISPOSAL - Schools should decide whether items published on the school website are retained as an archive or whether they should be deleted at the same time as the master copy	
	School Management	Minutes of Senior Management Team meetings and 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	
	School Management	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	
	School Management	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 + 3 years then REVIEW		SECURE DISPOSAL	

	School Management	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	
	School Management	Management of complaints	Yes	Date complaint resolved + 3 years then review. If the complaint relates to negligence or safeguarding then date the complaint resolved + 15 years. If the complaint relates to child sexual abuse then the complaint resolved + 75 years (this retention period will be reviewed once the government and the ICO have issued guidance about the implementation of the IICSA recommendations)		SECURE DISPOSAL	

	School Management	Newsletters and other items with a short operational use	No	Current year + 1 year		SECURE DISPOSAL - Schools should decide whether items published on the school website are retained as an archive or whether they should be deleted at the same time as the master copy	
	School Management	Records relating to the creation and publication of the school brochure or prospectus	No	Current year + 3 years. Schools should consider archiving one copy for historical reasons		STANDARD DISPOSAL	

Special Education Needs and Disabilities

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Special Education Needs and Disabilities	**Special Education Needs and Disabilities**	Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of birth of the pupil + 25 years	Limitation Act 1980	SECURE DISPOSAL	
	Special Education Needs and Disabilities	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then 6 years after legal action ended	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	SECURE DISPOSAL	IICSA recommendations awaited

	Special Education Needs and Disabilities	Advice and information provided to parents regarding educational needs	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then date legal action ceases + 6 years	Special Educational Needs and Disability Act 2001 Section 2	SECURE DISPOSAL	This retention period will be reviewed once the government and the Information Commissioner have published guidance about implementing the recommendations made by IICSA.
	Special Education Needs and Disabilities	Accessibility strategy	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then date legal action ceases + 6 years	Special Educational Needs and Disability Act 2001 Section 14	SECURE DISPOSAL	This retention period will be reviewed once the government and the Information Commissioner have published guidance about implementing the recommendations made by IICSA.

Teachers and Staff

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes

Teachers and Staff	**Disciplinary**	Disciplinary Proceedings: Oral warning	Yes	Date of warning + 6 months		SECURE DISPOSAL	Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice. Relevant to all disciplinary cases. The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line and defend him- or herself by saying "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.

	Disciplinary	Disciplinary Proceedings: Written warning level 1	Yes	Date of warning + 6 months		SECURE DISPOSAL	If warnings are placed on personal files, then they must be weeded from the file. Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice. Relevant to all disciplinary cases. The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line and defend him- or herself by saying "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.

	Disciplinary	Disciplinary Proceedings: Written warning level 2	Yes	Date of warning + 12 months		SECURE DISPOSAL	If warnings are placed on personal files, then they must be weeded from the file. Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice. Relevant to all disciplinary cases. The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line and defend him- or herself by saying "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept

	Disciplinary	Disciplinary Proceedings: Final warning	Yes	Date of warning + 18 months		SECURE DISPOSAL	If warnings are placed on personal files, then they must be weeded from the file. Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice. Relevant to all disciplinary cases. The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line and defend him- or herself by saying "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept

	Disciplinary	Disciplinary Proceedings: Case not found	Yes	If the incident is child protection related, then see IRMSTK29.1 otherwise dispose of at the conclusion of the case		SECURE DISPOSAL	
	Pay and Pensions	Records relating to the agreement of pay and conditions	No	Date pay and conditions superseded + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Payroll records	Yes	Date payroll run + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Payroll reports	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Payroll awards	Yes	Current year + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Payroll gross / net weekly or monthly	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Payslips copies	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1989	SECURE DISPOSAL	
	Pay and Pensions	Pay packet receipt by employee	Yes	Current year + 2 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Maternity pay records	Yes	Current year + 3 years	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	SECURE DISPOSAL	
	Pay and Pensions	Part time fee claims	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Overtime	Yes	Current year + 3 years		SECURE DISPOSAL	
	Pay and Pensions	National Insurance Schedule of payments	Yes	Current year + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Insurance	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Car allowance claims	Yes	Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Car mileage output	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1989	SECURE DISPOSAL	

	Pay and Pensions	Car loans	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Time sheets /clock cards / flexitime	Yes	Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Bonus sheets	Yes	Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	
	Pay and Pensions	Staff returns	Yes	Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1989	SECURE DISPOSAL	
	Pay and Pensions	Sickness records	Yes	Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1990	SECURE DISPOSAL	
	Pay and Pensions	Tax forms P6 /P11 / P11D / P35 / P45/ P46 / P48	Yes	Current year + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Personal bank details	Yes	Until superseded + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1990	SECURE DISPOSAL	
	Pay and Pensions	Income tax form P60	Yes	Current year + 6 years. Employees should keep your records for at least 22 months from the end of the tax year they relate to. The tax year runs from 6 April to the following 5 April, so keep paperwork until at least 31 January nearly two years later. For example, you should keep records relating to the tax year 2022/23 (which ends 5 April 2023) until 31 January 2025 or longer if you are self-employed.	Taxes Management Act 1970; Income and Corporation Taxes 1991	SECURE DISPOSAL	There is no harm in keeping them longer than strictly required. In particular, it is possible to go back up to four tax years to claim some reliefs and to claim a tax refund. In order to make those claims you need supporting evidence, so it would be helpful to keep records for at least four years after the end of the tax year.
	Pay and Pensions	Pension payroll	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1992	SECURE DISPOSAL	

	Pay and Pensions	Superannuation adjustments	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1993	SECURE DISPOSAL	
	Pay and Pensions	Superannuation reports	Yes	Completion of loan + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Members Allowance register	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1993	SECURE DISPOSAL	
	Pay and Pensions	Records relating to pension registrations	Yes	Date of last payment on the pension + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Management of the Teachers Pension Scheme	Yes	Date of last payment on the pension + 6 years		SECURE DISPOSAL	
	Pay and Pensions	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	From the end of the year in which the accounts were signed for a minimum of 6 years	Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103) Regulation 15	SECURE DISPOSAL	
	Recruitment	All records leading up to the appointment of a new Head Teacher	Yes	Length of appointment + 6 years		SECURE DISPOSAL	Academies do not necessarily have to employ people with qualified teacher status; only the SEN and designated LAC teacher must be qualified.
	Recruitment	All records leading up to the appointment of a new member of staff successful candidate	Yes	All relevant information should be added to the Staff Personal File (see below) and all other information retained for 6 months		SECURE DISPOSAL	
	Recruitment	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	

	Recruitment	Pre-employment vetting information DBS Checks	Yes	Schools do not have to keep copies of DBS certificates in order to fulfil the duty of maintaining the single central record. When a school chooses to retain a copy, there should be a valid reason for doing so and it should not be kept for longer than six months. When the information is destroyed, it must be done securely. Once a recruitment (or other relevant) decision has been made, we do not keep certificate information (e.g. DBS number) for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints or be for the purpose of completing safeguarding audits. If the school disposes of the certificate the following information should be retained in line with the DBS Code of Practice: Retain the following after the certificate is destroyed - 1. The date of issue of a disclosure; 2. The name of the subject; 3. The type of the disclosure requested; the position for which the Disclosure was requested; 4. The unique reference number of the Disclosure; 5. The details of the recruitment decision taken.	https://www.gov.uk/government/publications/dbs-update-service-employer-guide/dbs-update-service-employer-guide DBS Update Service Employer Guide June 2014; Keeping Children Safe in Education.2018 (Statutory Guidance from Dept. of Education) Sections 73, 74	SECURE DISPOSAL	Academies are bound by the legislation that applies to independent schools NOT maintained schools.

	Recruitment	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 added to the Staff Personal File		SECURE DISPOSAL	
	Recruitment	Pre-employment vetting information. Evidence proving the right to work in the United Kingdom	Yes	Where possible, these copies of documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	An employers guide to right to work checks [Home Office May 2015] Last updated 27 April 2022.	SECURE DISPOSAL	Employers are required to take a clear copy of the documents which they are shown as part of this process
	Recruitment	Records relating to the employment of overseas teachers	Yes	Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years		SECURE DISPOSAL	

	Safeguarding	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded	Yes	Until the persons normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	Keeping children safe in education Statutory guidance for schools and colleges March 2015; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015 July 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942454/Working_together_to_safeguard_children_inter_agency_guidance.pdf. Keeping children safe in education Statutory guidance September 2021. Sections 132, 133 The updated guidance (see below) does not mention a time limit for retention, but GDPR must be borne in mind - for only as long as necessary Keeping children safe in education Statutory guidance for schools and colleges Part 1: Information for all school and college staff September 2018 Section 35. Record keeping All concerns, discussions and decisions made, and the reasons for those decisions, should be recorded in writing. If in doubt about recording requirements, staff should discuss with the designated safeguarding lead (or deputy)	SECURE DISPOSAL	The retention period will be reviewed once the guidance by the government and ICO about implementing the recommendations made by IICSA has been published.
	Staff Management	Staff Personal File, including employment contract and staff training records	Yes	Termination of employment + 6 years	Limitation Act 1980	SECURE DISPOSAL	
	Staff Management	Timesheets	Yes	Current year + 3 years		SECURE DISPOSAL	
	Staff Management	Absence record	Yes	Current year + 3 years		SECURE DISPOSAL	

	Staff Management	Sickness Absence Monitoring	Yes	Sickness records are categorised as sensitive data. There is a legal obligation under statutory sickness pay to keep records for sickness monitoring. Sickness records should be kept separate from accident records' (2003) It could be argued that where sickness pay is not paid then current year + 3 years is acceptable whilst if sickness pay is made then it becomes a financial record and current year + 6 years applies. The actual retention may depend on the internal auditors. Most seem to accept current year+ 3 years as being acceptable as this gives them, 'Benefits' and Inland Revenue time to investigate if they need to.		SECURE DISPOSAL	
	Staff Management	Annual appraisal/assessment records	Yes	Current year + 3 years		SECURE DISPOSAL	
	Staff Management	Records relating to the TUPE process	Yes	Date last member of staff transfers or leaves the organisation + 6 years		SECURE DISPOSAL	

	Staff Management	Training needs analysis	No	Current year + 1 year		SECURE DISPOSAL	
	Staff Management	Staff Training where the training leads to Continuing Professional Development	Yes	Length of time required by the professional body		SECURE DISPOSAL	
	Staff Management	Staff Training except where dealing with children, e.g. First Aid or Health and Safety	Yes	This should be retained on the personnel file		SECURE DISPOSAL	
	Staff Management	Staff Training where the training relates to children (e.g. safeguarding or other child related training)	Yes	Date of the training + 40 years		SECURE DISPOSAL	This retention period will be reviewed when the government and ICO have published guidance about how to implement the recommendations made by IICSA.
	Staff Management	Professional Development Plans	Yes	Life of the plan or plan superseded + 6 years		SECURE DISPOSAL	

Teaching and the Curriculum

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Teaching and the Curriculum	**Teaching and the Curriculum**	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	

	Teaching and the Curriculum	Timetable	No	Academic 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	
	Teaching and the Curriculum	Class record books	No	Academic 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	
	Teaching and the Curriculum	Mark books	No	Academic 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	
	Teaching and the Curriculum	Record of homework set	No	Academic 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	

	Teaching and the Curriculum	Pupils work	Yes	Where possible, work should be returned to the pupil at the end of the academic year. If this is not the schools policy, then current year + 1 year		SECURE DISPOSAL	

Transport (Educational)

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Transport (Educational)	**Transport (Educational)**	The process of acquisition and disposal of vehicles through lease or purchase, e.g., contracts/leases, quotes, approvals	No	Disposal of the vehicle + 6 years	Limitation Act 1980	SECURE DISPOSAL	
	Transport (Educational)	The process of managing allocation and maintenance of vehicles, e.g., lists of who was driving the vehicles and when, and maintenance	No	Disposal of the vehicle + 6 years	Limitation Act 1981	SECURE DISPOSAL	
	Transport (Educational)	Service logs and vehicle logs	No	Life of the vehicle, then either to be retained for 6 years by school or to be returned to lease company	Limitation Act 1982	SECURE DISPOSAL	
	Transport (Educational)	GPS tracking data relating to the vehicles	No	Current year + 12 months	Limitation Act 1983	SECURE DISPOSAL	

	Transport (Educational)	Tachograph: Analogue and electronic including driver's cards	Yes	Current year + 12 months	Transport Act 1968 Chapter 73 Sections 96, 98, 99, 103. Passenger and Goods Vehicles (Recording Equipment) Regulations 2005 SI 2005 No 1904. Passenger and goods Vehicles (Recording Equipment) (downloading and Retention of Data) Regulations 2008 SI 2008 No 198. EC Regulation 561/2006 EC or AETR rules may also apply includes digital recording equipment	SECURE DISPOSAL	
	Transport (Educational)	Driver's records book	Yes	12 months from date of return of book to employer or in the case of owner driver 12 months from date of completion of book or it ceased to be used Driver to retain book for 14 days after all weekly record sheets have been used.	Transport Act 1968 Chapter 73 Sections 96, 98, 99, 103. Drivers' Hours (Goods Vehicles) (Keeping of Records) Regulations 1987. SI 1987 No.1421. Regulation 11 Preservation of driver's record books.	SECURE DISPOSAL	
	Transport (Educational)	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]	

Welfare

Category	Sub-Category	Retention Period Description	Personal Information	Retention Period	Statutory Provisions	Disposal	Notes
Welfare	**Welfare**	Family Liaison Officers and Home School Liaison Assistants: Day Books	Yes	Current year + 2 years then review		SECURE DISPOSAL	
	Welfare	Family Liaison Officers and Home School Liaison Assistants: 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		SECURE DISPOSAL	
	Welfare	Family Liaison Officers and Home School Liaison Assistants: Referral forms	Yes	While the referral is current		SECURE DISPOSAL	
	Welfare	Family Liaison Officers and Home School Liaison Assistants: Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy		SECURE DISPOSAL	
	Welfare	Family Liaison Officers and Home School Liaison Assistants: Contact database entries	Yes	Current year then review, if contact is no longer active then destroy		SECURE DISPOSAL	
	Welfare	Family Liaison Officers and Home School Liaison Assistants: Group Registers	Yes	Current year + 2 years		SECURE DISPOSAL	

	Welfare	Accessibility Plan relating to individual pupils	Yes	The plan should be included on the pupil file	Limitation Act 1980	SECURE DISPOSAL	
	Welfare	Child protection information held on pupil file	Yes	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file	Keeping children safe in education Statutory guidance for schools and colleges 2018; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018	SECURE DISPOSAL	This retention period will be reviewed when the government and ICO have published guidance about the implementation of the recommendations made by IICSA.
	Welfare	Child protection information held in separate files	Yes	Date of birth 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 LA Social Services record	Keeping children safe in education Statutory guidance for schools and colleges 2018; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018	SECURE DISPOSAL these records MUST be shredded	This retention period will be reviewed when the government and ICO have published guidance about the implementation of the recommendations made by IICSA.
	Welfare	Correspondence relating to authorised absence	Yes	Current academic year + 2 years	Education Act 1996 Section 7	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.