HILLVIEW
SCHOOL FOR GIRLS

Data Protection and FOI Policy

Including

Photographs of Children

Subject Access Requests

Records Retention Schedule

CONTENTS

INTRODUCTION

1. Hillview School for Girls ("the Academy") collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the Academy in order provide education and associated functions. The Academy may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (UK GDPR) and other related legislation.

2. The UK GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information) and if this is the case, it does not matter whether the information is located in a different physical location.

3. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed every 3 years.

DEFINITIONS

Personal Data

'Personal data' is any information relating to an individual that identifies an individual (directly or indirectly) and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1].

Special Category Data

A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

a) race or ethnic origin;

b) political opinions;

c) religious or philosophical beliefs;

d) trade union membership;

e) physical or mental health;

f) an individual's sex life or sexual orientation;

[1] For example, if asked for the number of female employees and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

g) genetic or biometric data for the purpose of uniquely identifying a natural person.

h) Personal data relating to criminal offences and convictions.

Special Category information is given special protection and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Academy does not intend to seek or hold special category personal data about staff or students except where the Academy has been notified of the information, or it comes to the Academy's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Academy their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

Data Subject

An identified or identifiable individual about whom we hold personal data.

Data Controller

The organisation storing and controlling the personal data (i.e. the Academy).

THE DATA PROTECTION PRINCIPLES

1. The six data protection principles as laid down in the UK GDPR are followed at all times:

    i. personal data shall be processed fairly, lawfully and in a transparent manner and processing shall not be lawful unless one of the processing conditions can be met;

    ii. personal data shall be collected for specific, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those purposes;

    iii. personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;

    iv. personal data shall be accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that is inaccurate is erased or rectified without delay;

v. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

vi. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

2. In addition to this, the Academy is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in Appendices 2 and 3).

3. The Academy is committed to complying with the principles in 3.1 at all times.

This means that the Academy will:

i. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

ii. be responsible for checking the quality and accuracy of the information;

iii. regularly review the records held to ensure that information is not held longer than is necessary and that it has been held in accordance with the data retention policy;

iv. ensure that when information is authorised for disposal it is done appropriately;

v. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and follow the relevant security policy requirements at all times;

vi. share personal information with others only when it is necessary and legally appropriate to do so;

vii. set out clear procedures for responding to requests for access to personal information known as subject access requests;

viii. report any breaches of the UK GDPR in accordance with the procedure in Appendix 5.

APPENDIX 1

CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

1. The individual has given consent that is specific to the particular type of processing activity and that consent is informed, unambiguous and freely given.

2. The processing is necessary for the performance of a contract to which the individual is a party or is necessary for the purpose of taking steps with regards to entering into a contract with the individual at their request.

3. The processing is necessary for the performance of a legal obligation to which we are subject.

4. The processing is necessary to protect the vital interests of the individual or another.

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 us.

6. The processing is necessary for a legitimate interest of the Academy or that of a third party, except where this interest is over-ridden by the rights and freedoms of the individual concerned.

APPENDIX 2

USE OF PERSONAL DATA BY THE ACADEMY

1. The Academy holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the **Data Protection Principles** as outlined on page 5.

Students

2. The personal data held regarding students includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and photographs.

3. The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care and to assess how well the Academy as a whole is doing, together with any other uses normally associated with this provision in a school environment.

4. The Academy may make use of limited personal data (such as contact details) relating to students and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with students of the Academy, but only where consent has been provided to this.

5. In particular, the Academy may:

   i. transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the Academy but only where consent has been obtained first;

   ii. make personal data, including special category personal data, available to staff for planning curricular or extra-curricular activities;

   iii. keep the student's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the student's first year at the Academy to their previous school;

   iv. Use photographs of students in accordance with this policy.

6. Any wish to limit or object to any use of personal data should be notified to the School Business Manager (SBM) in writing, which notice will be acknowledged by the Academy in writing. If, in the view of the SBM, the objection cannot be maintained, the individual will be given written reasons why the Academy cannot comply with their request.

Staff

1. The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs.

2. The data is used to comply with legal obligations placed on the Academy in relation to employment and the education of children in a school environment. The Academy may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

3. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

4. Any wish to limit or object to the uses to which personal data is to be put should be notified to the Human Resources Manager (HRM) who will ensure that this is recorded and adhered to if appropriate. If the HRM is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Academy cannot comply with their request.

Other Individuals

1. The Academy may hold personal information in relation to other individuals who have contact with the school, trustees, members of the Academy Trust, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

SECURITY OF PERSONAL DATA

1. The Academy will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the UK GDPR. The Academy will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

2. For further details as regards security of IT systems, please refer to the ICT Policy.

APPENDIX 3

DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

1. The following list includes the most usual reasons that the Academy will authorise disclosure of personal data to a third party:

i. To give a confidential reference relating to a current or former employee, volunteer or student;

ii. for the prevention or detection of crime;

iii. for the assessment of any tax or duty;

iv. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation imposed by contract);

v. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

vi. for the purpose of obtaining legal advice;

vii. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

viii. to publish the results of public examinations or other achievements of students of the Academy;

ix. to disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

x. to provide information to another educational establishment to which a student is transferring;

xi. to provide information to the Examination Authority as part of the examination process; and

xii. to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

2. The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

3. The Academy may receive requests from third parties (i.e. those other than the data subject, the Academy and employees of the Academy) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Academy.

4. All requests for the disclosure of personal data must be sent to the SBM, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

APPENDIX 4

CONFIDENTIALITY OF STUDENT CONCERNS

1. Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Academy will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Academy believes disclosure will be in the best interests of the student or other students.

APPENDIX 5

SUBJECT ACCESS REQUESTS

1. Anybody who makes a request to see any personal information held about them by the Academy is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).

2. All requests should be sent to the SBM within 3 working days of receipt and must be dealt with in full without delay and at the latest within one month of receipt.

3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The SBM must, however, be satisfied that:

   (a) the child or young person lacks sufficient understanding; and
   (b) the request made on behalf of the child or young person is in their interests.

4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Academy must have written evidence that the individual has authorised the person to make the application and the SBM must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

6. A subject access request must be made in writing. The Academy may ask for any further information reasonably required to locate the information.

7. An individual only has the automatic right to access information about themselves and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

8. All files must be reviewed by the SBM before any disclosure takes place. Access will not be granted before this review has taken place.

9. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A

copy of the full document and the altered document should be retained, with the reason why the document was altered.

10. If a subject access request is considered manifestly unfounded, for example to coerce the school into giving some form of benefit to the data subject or is malicious in intent to harass the school or an employee or trustee of the school with no purpose other than to cause disruption, the SBM can refuse to comply with the request.

11. If a subject access request is considered manifestly excessive such as the nature of the information sought or is a repeat of an earlier request which has been complied with, the SBM can refuse to comply with the request.

APPENDIX 6

EXEMPTIONS TO ACCESS BY DATA SUBJECTS

1. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

2. There are other exemptions from the right of subject access. If we intend to apply any of them to a request, such as seeking data about an individual or individuals other than the person making the request about their own data then we will usually explain which exemption is being applied and why.

APPENDIX 7

OTHER RIGHTS OF INDIVIDUALS

1. The Academy has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following section sets out how the Academy will comply with the rights to:

a) object to processing;

b) rectification;

c) erasure; and

d) data portability.

Right to object to processing

1. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

2. Where such an objection is made, it must be sent to the SBM within 2 working days of receipt and the SBM will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

3. The SBM shall be responsible for notifying the individual of the outcome of their assessment within 14 of working days of receipt of the objection.

Right to rectification

1. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the SBM within 2 working days of receipt and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable and the individual notified.

2. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

3. An individual also has a right to have incomplete information completed by providing the missing data and any information submitted in this way shall be updated without undue delay.

Right to erasure

1. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

(a) where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
(b) where consent is withdrawn and there is no other legal basis for the processing;
(c) where an objection has been raised under the right to object and found to be legitimate;
(d) where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
(e) where there is a legal obligation on the Academy to delete.

2. The SBM will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data and this data has been passed to other data controllers and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

1. In the following circumstances, processing of an individual's personal data may be restricted:

a) where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data;

b) where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure;

c) where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

d) where there has been an objection made under confidentiality of student concerns (see Appendix 4) pending the outcome of any decision.

Right to portability

1. If an individual wants to send their personal data to another organisation they have a right to request that the Academy provides their information in a structured, commonly used and machine readable format. As this right is limited to situations where the Academy is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the SBM within 2 working days of receipt and the SBM will review and revert as necessary.

APPENDIX 8

BREACH OF ANY REQUIREMENT OF THE UK GDPR

1. Any and all breaches of the UK GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the SBM

2. Once notified, the SBM shall assess:

   a) the extent of the breach;
   b) the risks to the data subjects as a consequence of the breach;
   c) any security measures in place that will protect the information;
   d) any measures that can be taken immediately to mitigate the risk to the individuals.

3. Unless the SBM concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Academy, unless a delay can be justified.

4. The Information Commissioner shall be told:

   a) details of the breach, including the volume of data at risk and the number and categories of data subjects;
   b) the contact point for any enquiries (which shall usually be the SBM);
   c) the likely consequences of the breach;
   d) measures proposed or already taken to address the breach.

5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the SBM shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it or measures have been taken to mitigate any risk to the affected individuals.

6. Data subjects shall be told:

   a) the nature of the breach;
   b) who to contact with any questions;
   c) measures taken to mitigate any risks.

7. The SBM shall then be responsible for instigating an investigation into the breach, including how it happened and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Headteacher and a decision made about implementation of those recommendations.

CONTACT

1. If anyone has any concerns or questions in relation to this policy, they should contact the SBM.

APPENDIX 9
PHOTOGRAPHIC POLICY

INTRODUCTION

1. The Academy is obliged to comply with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 when it takes or publishes photographs of its students. The Academy will always try to act in the best interest of the students and, as far as it legally can, it will take parental preferences into account.

2. The Data Protection Act gives children rights over their own data when they are considered to have adequate capacity to understand. Most children will reach this level of understanding at around age 12. For this reason, for most students in a secondary school, it will normally be up to the individual child to decide whether or not to be photographed. Where the school considers that the child does not have the capacity to make such a decision the school will act as it considers to be in the best interests of the child and in doing so will take account of any stated parental preference.

3. Ordinarily the following rules will apply to photographs in this school:

APPENDIX 10
Photographs for Internal Use

1. The Academy will take photographs for its own use. Usually these will be unnamed photographs and will generally be for internal school use but may also include photographs for publication, such as photos for the prospectus, or to show as slides at an event for parents. Unnamed photographs may also be used on display boards which can be seen by visitors to the Academy.

2. When the photograph is taken, the students will be informed that a photograph is being taken and told what it is for so that they can object if they wish.

3. If the Academy wants to use named photographs, then it will obtain specific consent first. For most students this will be student consent as explained above but parental wishes will be taken into account.

Media Use

1. The Academy will give proper consideration to the interests of its students when deciding whether to allow external organisations to take photographs or to film.

2. When the media are allowed to be present in the Academy or at Academy events, this will be on the condition that they observe this policy.

3. Where the media are allowed to be present at a particular event the Academy will make sure that students and their parents or carers are informed of the media presence. If no objection is received, then the Academy will assume that unnamed photographs may be published.

4. If the media entity wants to publish named photographs, then they must obtain specific consent from those students with capacity to consent or the parents of those without capacity. The Academy will require the media entity to check with the Academy before publication so that the school can check that any objections have been taken into account.

Family Photographs at School Events

1. It shall be at the discretion of the school whether photographs may be taken at a school event.

2. Family and friends taking photographs for the family album will not be covered by Data Protection legislation.
3. Where the Academy decides to allow such photography, the family and friends will be asked not to publish any photographs showing children other than their own on the internet.

APPENDIX 11

FREEDOM OF INFORMATION

INTRODUCTION

1. The Academy is subject to the Freedom of Information Act 2000 (FOI) as a public authority and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

WHAT IS A REQUEST UNDER FOI

1. Any request for any information from the Academy is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

2. In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the SBM.

3. All other requests should be referred in the first instance to the SBM, who may allocate another individual to deal with the request. This must be done promptly and in any event within 3 working days of receiving the request.

4. When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public and so once it has been released to an individual, anyone can then access it and you cannot restrict access when releasing by marking the information “confidential” or “restricted”.

TIME LIMIT FOR COMPLIANCE

1. The Academy must respond as soon as possible and in any event within 20 working days of the date of receipt of the request. For an Academy, a “working day” is one in which students are in attendance, subject to an absolute maximum of 60 calendar days to respond.

APPENDIX 12

PROCEDURE FOR DEALING WITH A REQUEST

1. When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the SBM, who may reallocate to an individual with responsibility for the type of information requested.

2. The first stage in responding is to determine whether or not the Academy "holds" the information requested. The Academy will hold the information if it exists in computer or paper format. Some requests will require the Academy to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Academy is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested and offered the opportunity to refine their request. For example, if a request required the Academy to add up totals in a spread sheet and release the total figures, this would be information "held" by the Academy. If the Academy would have to go through a number of spreadsheets and identify individual figures and provide a total, this is likely not to be information "held" by the Academy, depending on the time involved in extracting the information.

3. The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

a) Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

b) Section 22 – information that the Academy intends to publish at a future date;

c) Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

d) Section 36 – information which, in the opinion of the chair of trustees of the Academy, would prejudice the effective conduct of the Academy. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion;

e) Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

f) Section 40 (1) – the request is for the applicants' personal data. This must be dealt with under the subject access regime in the Data Protection Act (DPA), detailed in Appendix 5;

g) Section 40 (2) – compliance with the request would involve releasing third party personal data and this would be in Breach of the **DPA Principles** as set out on page 5;

h) Section 41 – information that has been sent to the Academy (but not the Academy's own information) which is confidential;

i) Section 43 – information that would prejudice the commercial interests of the Academy and / or a third party;

RESPONDING TO A REQUEST

1. When responding to a request where the Academy has withheld some or all of the information, the Academy must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

2. The letter should end by explaining to the requestor how they can complain by reference to the Academy Complaints Policy.

CONTACT

1. Any questions about this policy should be directed in the first instance to the SBM.

APPENDIX 13
DOCUMENT RETENTION

INTRODUCTION

1. The main aim of this policy is to enable the Academy to manage our records effectively and in compliance with data protection and other regulation. As an organisation we collect, hold, store and create significant amounts of data and information and this policy provides a framework of retention and disposal of categories of information and documents.

2. The Academy is committed to the principles of data protection including the principle that information is only to be retained for as long as necessary for the purpose concerned.

3. The table below sets out the main categories of information that we hold, the length of time that we intend to hold them and the reason for this.

4. For information, the Appendix sets out the legal requirements for certain categories of document.

5. Section 2 of this policy sets out the destruction procedure for documents at the end of their retention period. The SBM shall be responsible for ensuring that this is carried out appropriately and any questions regarding this policy should be referred to them.

6. If a document or piece of information is reaching the end of its stated retention period, but you are of the view that it should be kept longer, please refer to the SBM, who will make a decision as to whether it should be kept, for how long and note the new time limit and reasons for extension.

APPENDIX 14

DELETION OF DOCUMENTS

1. When a document is at the end of its retention period, it should be dealt with in accordance with this policy.

Confidential waste

1. This should be shredded using the shredder in the Reprographics Room. Otherwise, large volumes of confidential waste should be placed in confidential waste sacks available from the main office.

2. Anything that contains personal information should be treated as confidential.

3. Where deleting electronically, please refer to the Network Manager to ensure that this is carried out effectively.

Other documentation

1. Other documentation can be deleted or placed in recycling bins where appropriate.

Automatic deletion

1. Certain information will be automatically archived by the computer systems. Should you want to retrieve any information, or prevent this happening in a particular circumstance, please contact the Network Manager.

Individual responsibility

1. Much of the retention and deletion of documents will be automatic, but when faced with a decision about an individual document, you should ask yourself the following:

(a) Has the information come to the end of its useful life?

(b) Is there a legal requirement to keep this information or document for a set period? (Refer to Appendix 15 for more information)

(c) Would the information be likely to be needed in the case of any legal proceedings? In particular, is it potentially relevant to an historic child abuse enquiry? (Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?)

(d) Would the document be useful for the organisation as a precedent, learning document, or for performance management processes?

(e) Is the document of historic or statistical significance?

2. If the decision is made to keep the document, this should be referred to the SBM and reasons given.

APPENDIX 15

LEGAL TIME PERIODS FOR RETENTION OF DOCUMENTS

DOCUMENT TYPE	LEGISLATION / REASONS FOR RETENTION	REQUIREMENT
COMPANY RECORDS		
Company Articles of Association, Rules / bylaws	Companies Act 2006 Charities Act 2011	Permanent
Academy funding agreement and any supplemental agreements	Charities Act 2011	Permanent
Trustee / director minutes of meetings and written resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years
Members' meetings etc. Minutes / resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years
Documents of clear historical / archival significance	Data Protection regulation	Permanent if relevant data protection regulation provisions are met. At the time of writing the Data Protection Bill contains relevant provisions but these are expected to change as the Bill goes through the parliamentary process. Legal advice should be obtained once the Data Protection Act 2018 is published.
Contracts e.g. with suppliers or grant makers	Limitation Act 1980	Length of contract term plus 6 years
Contracts executed as deeds	Limitation Act 1980	Length of contract term plus 12 years

IP records and legal files re provision of service	Limitation Act 1980	Recommended: Life of service provision or IP plus 6 years

TAX AND FINANCE		
Annual accounts and review (including transferred records on amalgamation)	Companies Act 2006 Charities Act 2011	Minimum 6 years Recommended: permanent record
Tax and accounting records	Finance Act 1998 Taxes Management Act 1970	6 years from end of relevant tax year
Information relevant for VAT purposes	Finance Act 1998 and HMRC Notice 700/21	Minimum 6 years from end of relevant period
Banking records / receipts book/sales ledger	Companies Act 2006 Charities Act 2011	6 years from transaction
EMPLOYEE / ADMINISTRATION	See generally ICO Employment Practices Code	
Payroll / Employee / Income Tax and NI records: P45; P6; PIID; P60, etc.	Taxes Management Act 1970 / IT (PAYE) Regulations	6 years from end of current year
Maternity pay	Statutory Maternity Pay Regulations	3 years after the end of the tax year
Sick pay	Statutory Sick Pay (General) Regulations	3 years after the end of the tax year
National Minimum wage records	National Minimum Wage Act	3 years after the end of the tax year

Foreign national ID documents	Immigration (Restrictions on Employment) Order 2007 Independent School Standards Regulations	Minimum 2 years from end of employment
HR files and training records	Limitation Act 1970 and Data Protection regulation	Maximum 6 years from end of employment
Records re working time	Working Time Regulations 1998 as amended	2 years
Job applications (CVs and related materials re unsuccessful applicants)	ICO Employment Practices Code (Recruitment & Selection) Disability	Recommended: 6-12 months from your

	Discrimination Act 1995 & Race Relations Act 1976	notification of outcome of application
Pre-employment / volunteer vetting	ICO Employment Practice Code	6 months
Disclosure & Barring Service checks	Single Central Record Requirements under · for maintained schools: Regulations 12(7) and 24(7) and Schedule 2 to the School Staffing (England) Regulations 2009 and the School Staffing (England) (Amendment) Regulations 2013 (applied to student referral units through the Education (Student Referral Units) (Application of Enactments) (England) Regulations 2007); · for independent schools, (including academies and free schools and alternative provision academies and free schools): Part 4 of the Schedule to the Education (Independent School Standards) Regulations 2014;	Record only satisfactory / unsatisfactory result and delete other information. If copy is kept, not to be retained beyond 6 months See further DfE statutory Guidance ' Working Together to safeguard children' https://www.gov.uk/government/publications/working-together-to-safeguardchildren--2

INSURANCE		
Employer's Liability Insurance	Employers' Liability (Compulsory Insurance Regulation) 1998	40 years
Policies	Commercial	3 years after lapse
Claims correspondence	Commercial	3 years after settlement
HEALTH & SAFETY / MEDICAL		
General records	Limitation Act 1970	Minimum 3 years
Records re work with hazardous substances	Control of Hazardous Substances to Health Regulations 2002	Up to 40 years. Recommend: Permanent

Accident books / records and reports	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995	3 years after last entry or end of investigation
Medical Scheme documentation	Commercial	Permanent unless personal data is included
PREMISES / PROPERTY		
Original title deeds		Permanent / to disposal of property
Leases	Limitation Act 1980	12 years after lease has expired
Building records, plans, consents and certification and warranties etc.	Limitations Act 1980	6 years after disposal or permanent if of historical / archival interest. Carry out review re: longer retention, e.g. if possible actions against contractors
PENSION RECORDS	For all categories see:	
Records about employees and workers		

Records re the Scheme	Detailed Guidance for Employers – The Pensions Regulator	
Records re active members and opt in / opt out		
Trust Deed / Rules and HMRC approvals		
Trustees' Minutes and annual accounts		
Policies including investment policies		
STUDENTS		
Educational Record	Student information Regulations 2005 (maintained schools only) Same approach applied in academy context. Data Protection regulation	25 years from date of birth if this is the final school of the child but the student file should follow the student so it is likely to be difficult to justify the need for retention once the file has been passed to the student's new school
Child Protection information (on child's **file)**	"Keeping children safe in education Statutory guidance for schools and colleges September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children February 2017"	RETAIN UNTIL FURTHER RECOMMENDATIONS Subject to moratorium on destruction due to historic child abuse enquiry. See https://www.iicsa.org.uk/document/guidance-noteretention-instructions-anddata-protectionrequirements

Child Protection Information in other files	"Keeping children safe in education Statutory guidance for schools and colleges September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children February 2017"	RETAIN UNTIL FURTHER RECOMMENDATIONS Subject to moratorium on destruction due to historic child abuse enquiry. See https://www.iicsa.org.uk/document/guidance-noteretention-instructions-anddata-protectionrequirements
Special Educational Needs		
SEN files	Limitation Act 1980	Usually 25 years from date of birth of the student. If kept longer show good justification.
Education Health and Care Plans	Special Educational Needs and Disability Regulations 2014 Children and families Act 2014, part 3	25 years from date of birth of the student
Statements of Special Educational Needs (now historic)	Originally under Special Educational Needs and Disability Regulations 2001	25 years from date of birth of student unless passed to new school (usually on the student's file)
Attendance registers	Student Registration Regulations 2006 Regulation 14	For computerised registers retain until 3 years after the end of the school year
		during which the entry was made. This applies to every back up copy.
Other items e.g. curriculum related, photographs, video recordings	Case by case basis	

PARENTS	Student Registration Regulations 2006 For basic name and contact details. Otherwise usually operational in accordance with the statutory functions of the school	Usually, for the duration that the parent has a student at the school. Otherwise subject to case by case justification.
ALUMNI / ALUMNAE AND THEIR PARENTS		No legal clarity at present. Seek further advice when the Data Protection Act 2018 is in final form (likely to be April 2018)

Hillview School for Girls Trustees'
Data Protection & FOI Policy

Main compiler: Ali Newman

Date of approval by Trustees: July 2011

Updated: November 2023

Consulted: Audit and Risk Committee

Anticipated review date: November 2026

DDA Quality Check