



General Data Protection Regulation & Freedom of Information Policy

Date of Policy: Sept 2022

Date of Review: Sept 2024

Contents

Introduction

Part 1: Data Protection

1. Obtaining and Processing Data
2. Definitions
3. Purposes of Processing
4. Processing fairly, lawfully and transparently
5. Data Integrity
6. Subject Access
7. Data Security

Part 2: Freedom of Information

Statement of intent

1. Legal framework
2. Accepting requests for information
3. General right of access to information held by the school
4. The appropriate limit
5. Charging fees
6. Means by which communication is to be made
7. Providing advice and assistance
8. Publication scheme
9. Monitoring and review

Appendix C

- a) Model Publication Scheme

Part one

General Data Protection Regulations 2018

Introduction

Alleyne's Academy fully endorses and is committed to the General Data Protection Regulation May 2018 (GDPR). All staff and students are data subjects and both manual and electronic data relating to individuals are managed in accordance with the GDPR. All staff involved in the collection, processing and disclosure of personal data, are aware of their duties and responsibilities within this policy. The policy further outlines our response to Data Protection and provides a framework for managing and meeting requests.

1. Obtaining and Processing Data

- 1.1 Alleyne's Academy undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which data is held, the likely recipients of the data, who the data could be shared with and the data subject's rights of access to that data.

Information about the use of personal data is printed on appropriate data collection forms used by the Academy. These forms are sent annually to all parents/carers and additionally to staff to be updated together with a Privacy Statement.

2. Definitions

Processing Means any operation or set of operations which is performed on personal data, whether or not by automated means including collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, aligning, or combining, restricting erasing or destroying.

Data Controller Means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the means of processing personal data.

Data Processor Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Subject The identified or identifiable individual whose personal data is held or processed.

Personal Data Means any information relating to an identified or identifiable, natural person which can identify that individual directly or indirectly; for example name, id number, location data, online identifier such as username or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Parent/Carer Refers to the meaning given in the Education Act 1996 and includes any person who has parental responsibility for a child and for the purposes of this policy includes legal guardians (carers).

Legal disclosure The release of information from the computer to someone who requires

the information to do their job within the organisation, provided that the purposes of that information has been registered.

Illegal disclosure The release of information to someone who does not need it, or has no right to it, or one which falls outside the organisations registered purpose

3. Purposes of Processing

- 3.1 All information and data that can identify a living individual, held in any format (visual, verbal, paper, computer, microfilm, etc.) is safeguarded under GDPR. Alleyne's Academy is Registered with the Information Commissioner (Registration Number: ZA029582) under which are listed the purposes of the Academy's processing of personal data.
- 3.2 The lawful processing of data undertaken by the Academy as is necessary for "the performance of a task carried out in the public interest or the exercise of official authority vested in the Academy as Data Controller" in order to deliver education.
- 3.3 Where processing information exists beyond that outlined in 3.2 above, consent will be obtained from parents/carers for pupils under the age of 13 and/or those deemed incapable of understanding what they are consenting to, and pupils themselves over 13. This relates to such processing as the use of photographic images and biometric finger printing.
- 3.4 Under the 6 principles of the GDPR the Academy will only process personal data:
- fairly, lawfully and in a transparent manner
 - for specified, explicit and legitimate purposes
 - in a way that is adequate, relevant and limited
 - which is accurate and kept up-to-date
 - which is kept no longer than necessary
 - in a manner that ensures appropriate security of the personal data
- 3.5 The Academy is responsible for and can demonstrate compliance with these principles Under the GDPR the Academy has a Data Protection Officer and specific issues relating to data protection should be addressed to Anne Jones c/o Alleyne's Academy or a.jones@alleynes.staffs.sch.uk

4. Processing fairly, lawfully and in a transparent manner

- 4.1 The Academy has a Privacy Notice which details what information will be shared, with whom and for what purpose. This Privacy Notice is issued alongside the Data Collection Form every year and available to download from the Academy's website.
- 4.2 The Academy has a Consent Form which details the data for which permission is required.
- 4.3 Data is only kept until a pupil reaches the age of 25 when it will be deleted from the records, unless there are adequate legal reasons for keeping it longer. Pupils cannot request to be 'forgotten' until they reach 25 years of age.
Once a pupil leaves school, their data will be stored as it was on the date they left full time education at Alleyne's Academy. If at any stage in the future, it comes to light that data has changed this data will be updated. However, this data will no longer be processed and therefore no longer updated annually.

5. Data Integrity

5.1 Data Accuracy

Data will be as accurate and up to date as is reasonably possible. If a data subject informs the Academy of a change of circumstance their records will be updated as soon as practicable. A printout of data will be provided to all data subjects annually so they can check its accuracy and make any amendments. Where a subject challenges the accuracy of their data, Alleyne's Academy will immediately mark the record as potentially inaccurate and make the appropriate amendments.

5.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is held. In order to ensure compliance with this principle Alleyne's Academy will check records regularly for missing, irrelevant or seemingly excessive information and may contact the subjects to verify certain items of data.

5.3 Length of Time

Data held about individuals will not be kept for longer than necessary and for the purposes registered. A full schedule of the length of time documents will be kept is included in this document as [Appendix A](#).

After this time documents will be destroyed in a confidential manner by school personnel or organisations instructed to do so by the Academy under a confidential waste agreement.

6. Subject Access

The GDPR allows all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of request is in place. Where a subject access is received the Academy's policy is that:

- Requests from pupils will be processed as any subject access request outlined in 6.1 below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parent/carer
- Requests from parents/carers in respect of their own child will be processed as requests made on behalf of the data subject and the copy will be sent in a sealed envelope to the requesting parent/carer.

6.1 Processing Subject Access Requests

Requests for Access must be made in writing and addressed to the Data Protection Officer or alternatively a Subject Access Request form may be downloaded from the Academy's website. Completed forms should be returned to the Data Protection Officer at the Academy. Once we are satisfied that individuals meet the criteria for disclosure of data under the General Data Protection Regulations and have provided sufficient information, we will respond within one month from the date that we accept the application for processing.

6.2 Authorised Disclosure

Alleyne's Academy will, in general, only disclose data about individuals with their consent.

However there are circumstances under which the Academy may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the Academy to perform its statutory duties and obligations
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within the vicinity of the Academy.
- Staff data disclosed to relevant authorities, for example in respect of payroll and other administration matters such as student loans, pensions, occupational health, etc.

Only authorised staff will be allowed to make external disclosures of personal data. Data used within the Academy by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional, legitimately working within the Academy who need to know the information in order to do their work. We will not disclose anything on a pupils records which would be likely to cause serious harm to their physical or mental health or that of anyone else, including anything which suggests that they are or have been subject of at risk of child abuse.

7 Data Security

Alleynes Academy undertakes to ensure the security of personal data by the following general methods:

- encrypted usb sticks
- strong passwords, password protocol
- restriction of rights and access to SIMS –access given to those that require it to do their job

A deliberate breach of Policy will be treated as a disciplinary matter.

7.1 Physical Security

Appropriate building security measures are in place, such as alarms, window bars and deadlocks. Only authorised persons are allowed in to the Academy. Computers are locked when not in use, photocopying is not left on machines, printouts are locked away when not in use. Visitors to the Academy are required to sign in and out and wear a visitor's badge whilst in school and are, where appropriate, accompanied.

7.2 CCTV

The purpose of the CCTV system is for the security of the premises, the prevention, detection and investigation of criminal activity, trespass, vandalism and the safety of staff, students and visitors to the site. Static and remotely operated cameras enable this purpose. The CCTV is only viewed, when necessary, by a small list of registered people.

7.3 Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are undertaken

regularly. Computer files are backed up regularly.

7.4 Biometric Security

CRB Cunninghams software products hold Personal Data sourced from the school MIS (or created manually), the data is used to verify the identity of an individual at the point of service delivery via computer terminals, EPOS terminals, Coin & Note revaluation units, self-service kiosks, registration terminals, printers, lockers and other similar devices within the customers premises and subsequently allow them to use the services provided by that software product.

Biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored.

Biometric data is only held for as long the student/adult is at Alleyne's Academy.

7.5 Procedural Security

All new members of staff are given access to this Data Protection and Freedom of Information Policy as part of their induction programme and regular updates and refresher training are provided to all staff on an on-going basis.

Security arrangements are continually assessed and updated to ensure the latest affordable technology is applied and procedures are up to date. Guidance given to new members of staff as part of their induction programme in respect of basic standard security.

Any queries or concerns about security of data in the Academy in the first instance should be referred to the Data Protection Officer.

7.6 Data Breach Procedure

In the event of a suspected data breach, the DPO should be informed and the Data Breach Plan followed. See [Appendix B](#)

Part Two
Freedom of Information

Statement of intent

As an educational provider, our school has an obligation to publish a freedom of information statement, outlining how we will meet our duties under the Freedom of Information Act 2000 and associated regulations. The development and effective implementation of this policy fulfils that requirement.

More specifically, this policy outlines:

- How our school will respond to requests from individuals for access to information held about them.
- Our school's policy and procedures for the release and publication of private data and public records.
- Our school's policy and procedures for providing applicants with advice and assistance throughout the duration of their requests.

It also clarifies our position regarding the appropriate limit to the costs incurred by the school in obtaining any requested information, and on charging fees for its provision.

1. Legal framework

1.1. This policy has due regard to the following legislation:

- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- General Data Protection Regulation May 2018

1.2. This policy also has due regard to guidance, including, but not limited to, the following:

- Information Commissioner's Office 'Model publication scheme' 2016
- Information Commissioner's Office 'Duty to provide advice and assistance (section 16)' 2016
- Ministry of Justice 'Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000' 2009

2. Accepting requests for information

2.1. The school will only accept a request for information which meets all of the following criteria:

- It is in writing
- It states the name of the applicant and an address for correspondence
- It describes the information requested

2.2. A request will be treated as made in writing if it meets all of the following requirements:

- It is transmitted by electronic means
- It is received in legible form
- It is capable of being used for subsequent reference

2.3. The school will publish details of its procedures for dealing with requests for information on the website, which includes:

- A contact address and email address
- A telephone number
- A named individual to assist applicants with their requests

3. General right of access to information held by the school

3.1. Provided that the request complies with [section 2](#) of this policy, the school will, no later than 20 working days from receipt of the request, comply with its duty to:

- Confirm or deny to any person making a request for information to the school, whether it holds information of the description specified in the request.
- Provide the documentation, if the school confirms that it holds the requested information.

3.2. The school will not comply with section 3.1 of this policy where:

- The school reasonably requires further information to meet a freedom of information request, has informed the applicant of this requirement, but was not subsequently supplied with that further information.
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- A request for information is exempt under Section 2 of the Freedom of Information Act 2000.
- The cost of providing the information exceeds the appropriate limit.
- The request is vexatious.
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one.
- A fee notice was not honoured.

3.3. Where information is, or is thought to be, exempt, the school will, within 20 working days, give notice to the applicant which:

- States the fact.
- Specifies the exemption in question.

3.4. The information provided to the applicant will be in the format that they have requested, where possible.

3.5. Where it is not possible to provide the information in the requested format, the school will assist the applicant by discussing alternative formats in which it can be provided.

3.6. The information provided will also be in the language in which it is held, or another language that is legally required. If the school is required to translate any information, it will do so.

3.7. If, under relevant disability and discrimination regulations, the school is legally obliged to provide the information in other forms and formats, it will do so.

4. The appropriate limit

4.1. The school will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450.

4.2. When determining whether the cost of complying with a freedom of information request is within the appropriate limit, the school will take account only of the costs we reasonably expect to incur in relation to:

- Determining whether it holds the information.
- Locating the information, or a document which may contain the information.
- Retrieving the information, or a document which may contain the information.
- Extracting the information from a document containing it.

- Costs related to the time spent by any person undertaking any of the activities outlined in section 4.2 of this policy on behalf of the school, are to be estimated at a rate of £25 per person per hour.

4.3. Where multiple requests for information are made to the school within 60 consecutive working days of each other, either by a single person or by different persons who appear to be acting in concert, the estimated cost of complying with any of the requests is to be taken to be the total costs to the school of complying with all of them.

5. Charging fees

5.1. The school may, within 20 working days, give an applicant who has requested information from the school, a written notice stating that a fee is to be charged for the school's compliance.

5.2. Charges may be made for disbursements, such as the following:

- Photocopying
- Postage and packaging
- Costs directly incurred as a result of viewing information

5.3. Fees charged will not exceed the total cost to the school of:

- Informing the person making the request whether we hold the information.
- Communicating the information to the person making the request.

5.4. Where a fee is to be charged, the school will not comply with section 3 of this policy unless the requested fee is paid within a period of three months, beginning with the day on which the fees notice is given to the applicant.

5.5. The school will not take into account any costs which are attributable to the time spent by persons undertaking any of the activities mentioned in section 5.3 above.

5.6. When calculating the 20th working day in which to respond to a freedom of information request, the period beginning the day on which the fee notice is given to the applicant and ending with the day on which the fee is received, will be disregarded.

6. Means by which communication is to be made

6.1. Where, on making a request for information, the applicant expresses a preference for communication by any one of the following means, the school will, as far as is practicable, give effect to that preference:

- The provision to the applicant of a copy of the information in permanent form or in another form acceptable to the applicant.
- The provision to the applicant of a reasonable opportunity to inspect a record containing the information.

- The provision to the applicant of a digest, or summary of the information, in permanent form or in another form acceptable to the applicant.

7. Providing advice and assistance

7.1. The school will meet its duty to provide advice and assistance, as far as is reasonable, to any person who proposes to make, or has made, requests for information to the school.

7.2. The school may offer advice and assistance in the following circumstances:

- If an individual requests to know what types of information the school holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
- If a request has been made, but the school is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
- If a request has been refused, e.g. due to an excessive cost, and it is necessary for the school to assist the individual who has submitted the request.
-

7.3. The school will provide assistance for each individual on a case-by-case basis; examples of how the school will provide assistance include the following:

- Informing an applicant of their rights under the Freedom of Information Act 2000
- Assisting an individual in the focus of their request, e.g. by advising of the types of information available within the requested category
- Advising an applicant if information is available elsewhere and how to access this information
- Keeping an applicant informed on the progress of their request

7.4. In order to provide assistance as outlined above, the school will engage in the following good practice procedures:

- Make early contact with an individual and keep them informed of the process of their request.
- Accurately record and document all correspondence concerning the clarification and handling of any request.
- Give consideration to the most appropriate means of contacting the applicant, taking into account their individual circumstances.
- Discuss with the applicant whether they would prefer to receive the information in an alternative format, in cases where it is not possible to provide the information requested in the manner originally specified.
- Remain prepared to assist an applicant who has had their request denied due to an exemption.

7.5. The school will give particular consideration to what level of assistance is required for an applicant who has difficulty submitting a written request.

7.6. In circumstances where an applicant has difficulty submitting a written request, the school will:

- Make a note of the application over the telephone and then send the note to the applicant to confirm and return – the statutory time limit for a reply would begin here.
- Direct the individual to a different agency that may be able to assist with framing their request.
- **NB.** This list is not exhaustive and the school may decide to take additional assistance measures that are appropriate to the case.

- 7.7. Where an applicant's request has been refused either because the information is accessible by other means, or the information is intended for future publication or research, the school, as a matter of good practice, will provide advice and assistance.
- 7.8. The school will advise the applicant how and where information can be obtained, if it is accessible by other means.
- 7.9. Where there is an intention to publish the information in the future, the school will advise the applicant of when this publication is expected.
- 7.10. If the request is not clear, the school will ask for more detail from the applicant in order to identify and locate the relevant information, before providing further advice and assistance.
- 7.11. If the school is able to clearly identify the elements of a request, it will respond following usual procedures and will provide advice and assistance for the remainder of the request.
- 7.12. If any additional clarification is needed for the remainder of a request, the school will ensure there is no delay in asking for further information.
- 7.13. If an applicant decides not to follow the school's advice and assistance and fails to provide clarification, the school is under no obligation to contact the applicant again.
- 7.14. If the school is under any doubt that the applicant did not receive the advice and assistance, the school will re-issue it.
- 7.15. The school is not required to provide assistance where an applicant's request is vexatious or repeated, as defined under Section 14 of the Freedom of Information Act 2000.
- 7.16. The school is also not required to provide information where the cost of complying with a request exceeds the limit outlined in the Freedom of Information Act 2000. In such cases, the school will consider whether any information can be provided free of charge if the applicant refuses to pay the fee.
- 7.17. A record will be kept by the school of all the advice and assistance provided.

8. Publication scheme

8.1. The school will meet its duty to adopt and maintain a publication scheme which specifies the information which it will publish on the school website, and whether the information will be available free of charge or on payment.

8.2. The publication scheme will be reviewed and, where necessary, updated on an annual basis.

9. Monitoring and review

9.1. This policy will be reviewed on an annual basis, or in light of any changes to relevant legislation, by the Headteacher.

Appendix C

Model Publication Scheme

This scheme follows the model approved by the Information Commissioner's Office and sets out the classes of information which we publish or intend to publish; the format in which the information will be made available and whether the information is available free of charge or on payment.

1. Classes of information

Information that is available under this scheme includes:

- Who we are and what we do
- What we spend and how we spend it
- What are our priorities and how we are doing?
- How we make decisions
- Our policies and procedures
- Lists and registers
- The services we offer

Information which **will not** be made available under this scheme includes:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form, or notes, documents in older versions, emails or other correspondence.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

2. How to request information

Requested documents under this scheme will be delivered electronically where possible, but paper copies can be provided by contacting the school using the below contact details.

To enable us to process your request quickly, please mark all correspondence:

"FREEDOM OF INFORMATION REQUEST"

Documents can be translated under disability legislation into accessible formats where possible.

3. Charges

Documents contained in this scheme are free to view on the school website.

Single paper copies are also available free of charge to parents/carers and prospective parents/carers of the school.

Records Management Policy

Contents:

[Statement of intent](#)

1. [Legal framework](#)
2. [Responsibilities](#)
3. [Management of pupil records](#)
4. [Retention of pupil records and other pupil-related information](#)
5. [Retention of staff records](#)
6. [Retention of senior leadership and management records](#)
7. [Retention of health and safety records](#)
8. [Retention of financial records](#)
9. [Retention of other school records](#)
10. [Storing and protecting information](#)
11. [Accessing information](#)
12. [Digital continuity statement](#)
13. [Information audit](#)
14. [Disposal of data](#)
15. [Monitoring and review](#)

Statement of intent

Alleyne's Academy is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR.

1. Legal framework

- 9.2. This policy has due regard to legislation including, but not limited to, the following:
- General Data Protection Regulation
 - Freedom of Information Act 2000
 - Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- 9.3. This policy also has due regard to the following guidance:
- Information Records Management Society 'Information Management Toolkit for Schools' 2016
- 9.4. This policy will be implemented in accordance with the following school policies and procedures:
- ICT Policy

2. Responsibilities

- 9.5. The school has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
- 9.6. The Headteacher holds overall responsibility for this policy and for ensuring it is implemented correctly.
- 9.7. The Data Protection Officer (DPO) is responsible for the management of records at Alleyne's Academy.
- 9.8. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Headteacher.
- 9.9. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.
- 9.10. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

- 9.11. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.
- 9.12. The following information is stored on the front of a pupil record, and will be easily accessible:
- Forename, surname, gender and date of birth

- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate

9.13. The following information is stored inside the front cover of a pupil record, and will be easily accessible:

- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the school, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Any outside security issues, e.g. restricted access to student/records

9.14. The following information is stored in a secured pupil record, which can be accessed by authorised personnel:

- Admissions form
- Details of any SEND
- The record of transfer from previous school
- Fair processing notice – only the most recent notice will be included
- Annual written reports to parents
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any notes indicating child protection disclosures and reports
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes of records relating to complaints by parents/students/carers

9.15. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school's archive:

- Absence notes

- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
 - Correspondence with parents about minor issues, e.g. behaviour
- 9.16. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the Headteacher's PA's office – a note indicating this is marked on the pupil's file.
- 9.17. Hard copies of complaints made by parents or pupils are stored in a file in the Headteacher's PA's office – a note indicating this is marked on the pupil's file.
- 9.18. Actual copies of accident and incident information are stored separately in the secured archive room and held in line with the retention periods outlined in this policy. An additional copy may be placed in the pupil's file in the event of a major accident or incident.
- 9.19. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil may attend. However, if another pupil is mentioned, said pupil's identifying data will be redacted.
- 9.20. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed.
- 9.21. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 10 of this policy outlines how electronic records will be transferred.
- 9.22. If any pupil attends the school until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years.
- 9.23. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Retention of pupil records and other pupil-related information

- 9.24. The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.
- 9.25. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Secondary school admissions	The current academic year, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	The current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil's record	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed	Securely disposed of
Pupils' educational records		
Pupils' educational records	25 years after the pupil's date of birth	Securely disposed of
Public examination results	Added to the pupil's record	Returned to the examination board
Internal examination results	Added to the pupil's record	Securely disposed of
Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of
Attendance		
Attendance registers	25 years after the pupil's date of birth	Securely disposed of
Letters authorising absence	Current academic year, plus two years	Securely disposed of
SEND		

SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
Examination results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities		
Parental consent forms for school trips/work experience where no major incident occurred	Until the conclusion of the trip	Securely disposed of

Parental consent forms for school trips/work experience where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of
Home-School Liaison / Tuition		
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets	Current academic year	Reviewed and destroyed if no longer active
Contact database entries	Current academic year	Reviewed and destroyed if no longer required
Biometric Recording		
Biometric Fingerprint Consent Form	While student on roll	Deleted from system
CCTV	21 days	Deleted from system

5. Retention of staff records

9.26. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

9.27. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
Recruitment		

Records relating to the appointment of a new Headteacher	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, otherwise it will be securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of

Disciplinary and grievance procedures

Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file

Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

7.Retention of senior leadership and management records

9.28. The table below outlines the school’s retention periods for SLT and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing Body		
Agendas for Governing Body meetings	One copy alongside the original set of minutes	
Original, signed copies of the minutes of Governing Body meetings	Permanent	
Inspection copies of the minutes of Governing Body meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Reports presented to the Governing Body	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Meeting papers relating to the annual parents’ meeting	Date of meeting, plus a minimum of six years	Securely disposed of
Instruments of Government, including Articles of Association	Permanent	

Trusts and endowments managed by the Governing Body	Permanent	
Action plans created and administered by the Governing Body	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the Governing Body	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the Governing Body	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of
Headteacher and Senior Leadership Team (SLT)		
Log books of activity in the school maintained by the Headteacher	Date of last entry, plus a minimum of six years	Reviewed and securely disposed of
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the Headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
Records created by the Headteacher, Deputy Headteacher, Heads of Progress & Support and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and securely disposed of
Records created by the Headteacher, Deputy Headteacher, Heads of Progress & Support and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
School development plan	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

9.29. The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

9.30. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

8. Retention of financial records

9.31. The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

9.32. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Securely disposed of
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
Contract management		

All records relating to the management of contracts	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
School Fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School meals		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers (external contractor)	Current academic year, plus three years	Securely disposed of
School meals summary sheets (external contractor)	Current academic year, plus three years	Securely disposed of

9. Retention of other school records

9.33. The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

9.34. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the school	Permanent	
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
Maintenance		

All records relating to the maintenance of the school carried out by contractors	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	Securely disposed of
Operational administration		
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	Disposed of
Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of

10. Storing and protecting information

- 10.1. The DPO will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.
- 10.2. The DPO will liaise with Entrust to ensure a back-up of information is carried out on a regular basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
- 10.3. Where possible, backed-up information will be stored off the school premises.
- 10.4. Confidential paper records are kept in a locked archive room with restricted access.
- 10.5. Confidential paper records are not left unattended or in clear view when held in a location with general access.
- 10.6. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.
- 10.7. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.
- 10.8. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- 10.9. All electronic devices are password-protected to protect the information on the device in case of theft.
- 10.10. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 10.11. Staff and Governors do not use their personal laptops or computers for school purposes.

- 10.12. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 10.13. Emails do not contain sensitive or confidential information which would enable a subject to be identified.
- 10.14. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.
- 10.15. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- 10.16. Before sharing data, staff always ensure that:
- They have consent from data subjects to share it.
 - Adequate security is in place to protect it.
 - The data recipient has been outlined in a privacy notice.
- 10.17. All staff members will ensure there is no unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
- 10.18. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- 10.19. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the Site Manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Headteacher and extra measures to secure data storage will be put in place.
- 10.20. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 10.21. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

11. Accessing information

- 11.1. Alleyne's Academy is transparent with data subjects, the information we hold and how it can be accessed.
- 11.2. A GDPR folder is accessible by all staff under the U: drive which contains policies, privacy notices and current information. Hard copies are available on request.

- 11.3. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:
- Know what information the school holds and processes about them or their child and why.
 - Understand how to gain access to it.
 - Understand how to provide and withdraw consent to information being held.
 - Understand what the school is doing to comply with its obligations under the GDPR.
- 11.4. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.
- 11.5. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.
- 11.6. Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.
- 11.7. The school will adhere to the provisions outlined in the school's GDPR Data Protection Policy when responding to requests seeking access to personal information.

12. Digital continuity statement

- 12.1. The Digital Continuity Statement is accessible via the U: drive.

13. Information audit

- 13.1. The school conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:
- Paper documents and records
 - Electronic documents and records
 - Databases
 - Sound recordings
 - Video and photographic records
 - Hybrid files, containing both paper and electronic information
- 13.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
 - Questionnaires to staff members to identify information and information flows, etc.
 - A mixture of the above
- 13.3. The DPO is responsible for completing the information audit. The information audit will include the following:
- The school's data needs
 - The information needed to meet those needs
 - The format in which data is stored
 - How long data needs to be kept for
 - Vital records status and any protective marking
 - Who is responsible for maintaining the original document
- 13.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.
- 13.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Information Asset Register.
- 13.6. The information displayed on the Information Asset Register will be shared with the Headteacher for approval.

14. Disposal of data

- 14.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
- 14.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.
- 14.3. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.
- 14.4. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.
- 14.5. Where information must be kept permanently, this information is exempt from the normal review procedures

- 14.6. Where staff have consented to Biometric fingerprints, it will only be held for as long as the staff member is employed by Alleyne's Academy. After which it will be deleted.

15. Monitoring and review

- 15.1. This policy will be reviewed on an annual basis by the DPO in conjunction with the Headteacher.
- 15.2. Any changes made to this policy will be communicated to all members of staff and the Governing Body.

Data Breach Plan

