Freemen's

Learn, lead and make a difference

CITY OF LONDON FREEMEN'S SCHOOL

ASHTEAD, SURREY

Data Protection Policy

Version number	2.5
Name and appointment of owner / author	Oonagh O'Mahoney (Chief Operating Officer) / Anna Atkins (Director of HR)
Review Body	SLT and Finance, General Purposes & Estates Committee
Last updated	5th October, 2026
Reason for update	SLT review
Last reviewed by SLT	5th October, 2026
Last reviewed by Governors	15th October, 2025
Next SLT review due	September 2027
Next Governor review due	October 2027
Where available	School website, Freemen's Staff SharePoint site, Parent Portal, Governor Portal

This Policy is, in line with the advice from the Information Commission, reviewed annually by the School's SLT and, in addition, biennially by Governors. It should be read in conjunction with the School's *Complaints Policy* and *Data Retention Schedule*.

Contents

Data Protection Policy 1
General Statement of the Duties of the City and the School 3
The Data Protection Act 2018 3
Processing of Personal Data 5
Exemptions which Allow Disclosure of Personal Data to Third Parties 5
Use of Personal Information by the Schools 6
Accuracy of Personal Data 8
Security of Personal Data 8
Retention of Personal Data 8
Rights of Access by Data Subjects to their Personal Data 9
Requests for Access to Records (Subject Access Requests) 9
Responding to Requests for Access to Records 9
Authorisation of Access to Records on Behalf of a Child or Young Person 10
Disclosure of Information 11
Exemptions to Access by Data Subjects 12
Repeated Requests for Access to Records 13
Complaints 13
Contents 14
3. 1. Introduction 15
5. Biometric data use at Freemen's School 17
6. Associated Resources 17

Freemen's

Learn, lead and make a difference

CITY OF LONDON FREEMEN'S SCHOOL

ASHTEAD, SURREY

PUPIL & PARENT DATA PROTECTION POLICY

General Statement of the Duties of the City and the School

1. The City of London Corporation ('the City') is the data controller for the City of London Freemen's School ('the CLFS'), the City of London School ('the CLS'), the City of London School for Girls ('the CLSG') and the Guildhall Young Artists Division ('Junior Guildhall & Centre for Young Musicians') of the Guildhall School of Music & Drama. This Policy applies to personal information held and processed by the City of London Freemen's School for the purposes of the United Kingdom General Data Protection Regulations ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018")..

2. The City, and the Schools, are required to process personal data regarding pupils, their parents and guardians as part of their operation, and will take all reasonable steps to do so in accordance with this Policy, the UK GDPR and the DPA 2018). The City aims to have transparent systems for holding and processing written personal data. Any reference to personal data in this Policy includes reference to special category data. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

3. Any individual is entitled to request access to information relating to their personal data held by the schools. In this Policy any reference to pupils includes current, past or prospective pupils.

The Data Protection Act 2018

4. The City, and therefore each of the Schools, has the responsibility to comply with the DPA 2018.

5. The DPA 2018 applies to information relating to both "personal" and "special category" data.

6. **Personal Data** is defined in the DPA 2018 as information relating to and identifying a living individual ("data subject"). The Schools may process a wide range of personal data of pupils, their parents or guardians, as part of their operation. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject's privacy. Personal data includes facts, any expression of opinion about an individual and any indication of the intentions of anyone in respect of that individual. Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

7. **Special categories of personal data** means personal data which reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, generic biometric and health data, information relating to a data subject's sex life or sexual orientation, criminal convictions and alleged offences. It also includes biometric data (see appendix).

8. In order to comply with the DPA 2018 the School must comply with the six Data Protection Principles which state that personal data:

   i. Will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
   ii. Will be collected only for specified, explicit and legitimate purposes; and it must not then be further processed in any manner incompatible with those purposes.
   iii. Will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
   iv. Will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
   v. Will not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.

vi. Will be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9. **Processing** includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data.

Processing of Personal Data

10. Consent may be required for the processing of personal data unless the processing is necessary for the Schools to undertake their obligations to pupils and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the DPA 2018, will only be disclosed to third parties under the terms of this Policy or otherwise with the consent of the appropriate individual.

11. The rights in relation to personal data set out under the DPA 2018 are those of the individual to whom the data relates. The Schools will, in most cases, rely on parental or guardian consent to process data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is unreasonable in all the circumstances to rely on the parents' / guardian's consent. Parents should be aware that in such situations they may not be consulted.

12. Consent must be freely given, can be freely withdrawn and will generally be recorded by the individual's signed agreement.

Exemptions which Allow Disclosure of Personal Data to Third Parties

13. There are a number of exemptions in the DPA 2018 which allow disclosure of personal data to third parties, and the processing of personal data by the School and its employees, which would otherwise be prohibited under the DPA 2018. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely:

    (a) the data subjects have given their consent (with regard to special categories of data, this may require explicit, written consent, depending on the circumstances);
    (b) for the prevention or detection of crime;
    (c) for the assessment of any tax or duty;
    (d) where it is necessary to exercise a right or obligation conferred or imposed by law upon the City or the Schools (other than an obligation imposed by contract);
    (e) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
    (f) for the purpose of obtaining legal advice;

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

Use of Personal Information by the Schools

14. It is required under the DPA 2018 that the personal data held about pupils must only be used for specific purposes allowed by law. The School holds personal data on pupils. The personal data includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

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

16. The School may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School.

17. In particular, the School may:

(a) transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the School;
(b) with parental consent, make use of photographs of pupils in School publications and on the School website;
(c) with parental consent, disclose photographs and names of pupils to the media (or allow the media to take photographs of pupils) for promotional and congratulatory purposes where a pupil may be identified by name when the photograph is published e.g. where a pupil has won an award or has otherwise excelled;
(d) make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
(e) keep the pupil's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the school to their previous school.

18. Any wish to limit or object to any use of personal data should be notified to the COO of the relevant School in writing, which notice will be acknowledged by the School in writing. Parents who do not want their child's photograph or image to

appear in any of the School's promotional material, or be otherwise published, must also make sure their child knows this.

19. Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use the DPA 2018 will not apply e.g. where a parent takes a photograph of their child and some friends taking part in the School sports day.

20. The School may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the School) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA 2018 which allows disclosure applies (see paragraph 13); or where necessary for the legitimate interests of the individual concerned or the School.

21. The following are the most usual reasons that the School may have for passing personal data to third parties:

    (a) to give a confidential reference relating to a pupil;
    (b) to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend;
    (c) to publish the results of public examinations or other achievements of pupils of the School;
    (d) to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
    (e) to provide information to another educational establishment to which a pupil is transferring;
    (f) to provide information to the Examination Authority as part of the examinations process; and
    (g) to provide 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.

22. The DfE uses information about pupils 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 pupils 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.

23. Any wish to limit or object to any use of personal data by third parties, except as stated in paragraph 21 above, should be notified to the COO of the relevant School in writing, or to the relevant authority (the contact details for which can be supplied by the School).

24. Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

Accuracy of Personal Data

25. The City and the Schools will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the relevant School's COO in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Security of Personal Data

26. The City and the Schools will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this Policy and their duties under the DPA. The City and the Schools will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Retention of Personal Data

27. The Schools will have retention policies in place to ensure that personal data processed for any purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes.

Deletion of personal data

28. Where personal information is to be disposed of, the School will ensure that it is destroyed permanently and securely. This may involve the permanent removal of the information from the server so that it does not remain in a person's inbox, deleted items folder or recover deleted items folder, or, in the case of hard copies, shredding.

Rights of Access by Data Subjects to their Personal Data

29. Under the DPA 2018, individuals have a right of access to their personal data held by the City and the Schools. This is known as a "subject access request" and is subject to exemptions and constraints within the DPA 2018. Any request in writing will be responded to as long as satisfactory identification is given and the information request is clear.

Requests for Access to Records (Subject Access Requests)

30. A subject access request must be made in writing. Where the request is not complete or clear, or satisfactory identification has not been given, a request for clarification must be sent to the individual concerned within **two** working days of when the request is received by the School.

31. All requests for access to records must be placed on the relevant pupil's file, and the City's Information Compliance Team informed that the request has been received.

Responding to Requests for Access to Records

32. All requests for access to records must be passed to the Director of HR.

33. The Headmaster or, in his absence, the COO must authorise the applicant's request for access before **any** information is disclosed (see also paragraphs 39-43 below).

34. The School will take advice from the Information Compliance Team or the Comptroller and City Solicitor in relation to disclosure.

35. All SARs must be acknowledged. The School must respond to a SAR, subject to any exemptions or constraints to disclosure, within one calendar month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three calendar months of the date on which the request is received. The Director of HR will write to the individual within one month of receiving the original request to tell them if this is the case.

36. The DPA 2018 requires a response to a request to be given within **one calendar month** of the written request being received. The response period does not begin until:

    (a) a written application is received by anyone within the City of London Corporation (not when it has been passed on to and received by the Headmaster, COO, City's Information Compliance Team or the Comptroller and City Solicitor);

(b) the School has received sufficient information to enable it to identify the individual who is seeking access;
(c) the School has received sufficient information to enable it to access the information requested; and

37. Where the conditions set out in paragraph 36 are fulfilled, in responding to the request, the School must confirm whether personal data is being processed and where that is the case, give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data is or may be disclosed. The School must also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information. Finally, where processing results in automated decision making which evaluates matters relating to the data subject (for example, in the marking of multiple choice questions), the data subject should be informed and informed also of the logic involved in that decision-making.

38. Data subjects are not entitled to information where exemptions to the right of access apply (see paragraphs 56-60 below). Moreover, in these circumstances, the School must only give a notification to the data subject that no information has been identified which is required to be supplied under the DPA 2018.

Authorisation of Access to Records on Behalf of a Child or Young Person

39. A child or young person may appoint a person with parental responsibility for him or her to request access to their records. In such circumstances the School must have written evidence that the child or young person has authorised the person with parental responsibility to make the application.

40. The Headmaster or, in his absence, the COO will determine what information will be shared with the person with parental responsibility. Access to records will be refused in instances where, for example, information sharing may place a child at risk of significant harm or jeopardise police investigations into any alleged offence(s).

41. Where a child or young person does **not** have sufficient understanding to make his or her own request, a person with parental responsibility can make a request on their behalf. The Headmaster or, in his absence, the COO 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.

42. The School will only grant pupils' access to their personal data if, in the relevant School's reasonable belief, the pupil understands the nature of the request. It is generally

accepted that, by the age of 13, a child can be expected to have sufficient maturity to understand the nature of the request.

43. Where a pupil 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 School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Disclosure of Information

44. Any individual is, subject to exemptions and constraints within the DPA 2018, entitled to have access to all information specifically held about him or her where:

(a) it is automated data being personal data held or processed electronically, for example, on a computer, word processor, audio and video system or telephone logging system;
(b) it is manual data which consists of non-automated information such as paper or microfiche files or records, which record information as part of a relevant filing system. A relevant filing system is defined as a set of information relating to individuals and structured either by reference to individuals or specific criteria relating to those individuals, so that specific information relating to a particular individual is readily accessible in a way broadly equivalent to information accessed within a computerised system.

45. The personal data must be provided in permanent form (e.g. paper, microfiche, CCTV images) unless:

(a) the supply of such a copy is not possible;
(b) supplying it in permanent form would involve disproportionate effort (in which case another way of viewing the data must be agreed with the applicant); or
(c) the data subject agrees otherwise.

46. Only relevant documents from the pupil's file will be duplicated and disclosed to the applicant who, if requested, should be given a copy of the duplicated document.

47. An individual is not entitled to information where:

(a) exemptions to the right of access apply (see paragraphs 56-60 below); or
(b) another person, including any family member, has not given their written consent to disclose information that identifies them (**but** see paragraph 49 below) .

48. Information contained in an individual's records is likely to contain information about persons other than the individual. Generally, information about or identifying another person must not be disclosed to the individual seeking access to the information without that person's written consent.

49. There may be circumstances where the Headmaster or, in his absence, the COO considers it *reasonable in all the circumstances* to disclose information without the consent of the other person. For example, when the person cannot be traced.

50. In determining what is reasonable in all the circumstances it is necessary to have regard to:

    (a) any duty of confidentiality owed to the other person;
    (b) any steps taken with a view to seeking consent of the other person to the disclosure;
    (c) whether the other person is capable of giving consent; and
    (d) any express refusal of consent by the other person.

51. In instances where the Headmaster or, in his absence, the COO have decided information concerning other people, or their identities may not be disclosed, it is acceptable to blank out the relevant information.

52. There is also a general presumption in favour of disclosing personal data relating to individuals, where this information is integral to the personal data of the applicant. So, the records kept by teachers in the course of their employment in respect of pupils may be disclosable.

53. Any request by an individual for access to information held about them must be complied with subject to this paragraph and to the exemptions set out in paragraphs 56-60 below. The School may, however, make a request for more specific details of the information sought.

54. A request for access to files without the permission of the individual must be directed to the Information Compliance Team or the Comptroller and City Solicitor.

55. A record of the information disclosed in response to a request for access to information should be kept on the pupil's file, including details of any exemptions to disclosure relied upon (see paragraphs 56-60 below).

Exemptions to Access by Data Subjects

56. Confidential references given, or to be given by the Schools, are exempt from access. The Schools will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil.

57. It should be noted that confidential references received from other parties may also be exempt from disclosure, under the common law of confidence. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

58. Examination scripts, that is information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

59. Examination marks do not fall within an exemption as such. However, the one calendar month compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the School received the request (if all the necessary conditions set out in paragraph 36 are fulfilled), or one calendar month from the announcement of the examination results, whichever is the earlier.

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

Repeated Requests for Access to Records

61. Unless a reasonable period of time has lapsed between the compliance with one request and receipt of the next, under the DPA 2018 the School is not obliged to comply with subsequent identical or similar requests from that applicant.

Complaints

62. If an individual believes that the relevant School has not complied with this Policy or acted in accordance with the DPA they should utilise the School's *Complaints Policy*.

63. If the individual is still not satisfied, they may make representations to the Information Commission, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Telephone: 0303 123 1113.

Appendix

Biometric Data Policy

Contents

1. Introduction
2. What is biometric data?
3. What is an automated biometric recognition system?
4. What does data processing mean?
5. Biometric data use at Freemen's School
6. Frequently Asked Questions
7. Associated Resources
8. Equality Impact Assessment

For the purposes of this policy, the term 'parent' refers to all persons with parental responsibility.

3. 1. Introduction

1.1 Schools and colleges that use pupils' biometric data (see 1 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA).

1.2 Where the data is to be used as part of an automated biometric recognition system (see 2 below), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

1.3 The City of London Freemen's School (the School) will ensure that each parent of a child is notified of the School's intention to use the child's biometric data (see 1 below) as part of an automated biometric recognition system.

1.4 The written consent of at least one parent will be obtained before the data is taken from the child and used (i.e. 'processed' – see 3 below). This applies to all pupils in schools and colleges under the age of 18. In no circumstances will a child's biometric data be processed without written consent.

1.5 The School will not process the biometric data of a pupil (under 18 years of age) where:

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- No parent has consented in writing to the processing; or
- A parent has objected in writing to such processing, even if another parent has given written consent.

1.6 The School will provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

2. What is biometric data?

2.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can

include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2.2 Biometric data is classified as Special Category data under the GDPR and DPA. A lawful basis for processing under Article 9 of GDPR must be identified by the school. For the purposes of this document, the lawful basis is Article 9(2)(a) Consent.

2.3 Biometric data must be obtained, used and stored in accordance with the GDPR and DPA.

2.4 In line with GDPR requirements, a Privacy Impact Assessment must be carried out before the biometric data system is implemented, assessing any risks to data subjects and the measures the School will take to minimise the risks.

2.5 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 1998 and 2018.

3. What is an automated biometric recognition system?

3.1 An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

3.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1) above.

4. What does data processing mean?

4.1 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- Storing pupils' biometric information on a database system; or
- Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

5. Biometric data use at Freemen's School

5.1 The School uses biometric data for Sixth Form registration where parents have given permission for this. Parental permission is recorded on each student's record on Schoolbase. This information, along with all other data on the student record, is sent to parents regularly to check and review. The biometric systems use an algorithm-based scan, which reads between 50 and 130 points on the finger/thumb. Only the algorithm is stored, not the actual fingerprint. This is stored securely within a controlled access server on the school's site.

5.2 Written parental consent to take and use biometric data is sought for each child on admission to the school.

6. Associated Resources

- DfE guidelines for Protection of Biometric Information of Children in Schools https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/bi ometrics_advice_revi sed_12_12_2012.pdf
- DfE guidelines for schools on communicating with parents and obtaining consent: https://www.gov.uk/government/publications/dealing-with-issues-relating-to-parentalhttps://www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibilityresponsibility
- British Standards Institute guide to biometrics: http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r