



# Data Protection Policy

| Date of Review | Reason for Review | Model or School Specific Policy | Responsibility | Date Ratified | CoC Initials | Name of Committee | Date of next scheduled review |
|----------------|-------------------|---------------------------------|----------------|---------------|--------------|-------------------|-------------------------------|
| Mar 2021       | Scheduled Review  | Model                           | Data Manager   | March 2021    |              | FGB               | Mar 2022                      |



## Contents

|  |    |
|--|----|
| 1. Purpose .....   | 3  |
| 2. Data Protection Principles .....                        | 3  |
| 3. Responsibilities .....                                  | 3  |
| 3.1 Responsibilities of Staff .....                        | 5  |
| 4. Privacy Notice .....                                    | 5  |
| 5. Processing, Disclosure and Sharing of Information ..... | 5  |
| 5.1 Images and Biometric Data .....                        | 6  |
| 6. Requests for Access to Information .....                | 7  |
| 7. Complaints and Breach Notification .....                | 7  |
| 8. Contact Information .....                               | 7  |
| 9. Associated Policies .....                               | 7  |
| Appendix 1: Template Privacy Notice (Pupils).....          | 9  |
| Appendix 2: Template Privacy Notice (Staff).....           | 14 |
| Appendix 3: Pupil Photograph & Video Consent Form .....    | 21 |
| Appendix 4: Staff Photograph & Video Consent Form .....    | 23 |
| Appendix 5: Data Breach Procedure .....                    | 25 |
| Appendix 6: Personal Data Incident Reporting Form .....    | 29 |



## 1. Purpose

The EU's General Data Protection Regulation (the "**GDPR**"), as well as domestic legislation that remains in place until the GDPR comes into force on 25 May 2018 or that enhances or replaces the GDPR from time to time, lay down rules to protect personal privacy and uphold individuals' rights (the "**Data Protection Rules**"). The Data Protection Rules apply to anyone who "processes" (e.g. handles or has access to) individuals' personal data.

This Policy is intended to ensure that personal information is processed properly and securely and in accordance with the Data Protection Rules. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

## 2. Data Protection Principles

The GDPR provides seven data protection principles, which the School will follow to ensure good data handling:

- 1) **Lawfulness, fairness and transparency:** Personal data shall be processed fairly, lawfully and in a transparent manner;
- 2) **Purpose limitation:** Personal data shall be obtained only for one or more specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes (unless it is for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes);
- 3) **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary for its processing purposes;
- 4) **Accuracy:** Personal data shall be accurate and where necessary kept up to date, and every reasonable step must be taken to ensure that data which is inaccurate is erased or rectified without delay;
- 5) **Storage limitation:** Personal data shall not be kept in a form which allows the identification of individuals for longer than is necessary for the purpose for which it is processed (unless it is solely for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes and appropriate security measures have been implemented);
- 6) **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures its security, using appropriate technical and organisational security measures, in order to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- 7) **Accountability:** The organisation in control of the data is responsible for compliance with the other principles and must be able to demonstrate compliance with them.

## 3. Responsibilities

The School is the legal entity responsible for the processing of personal data and is therefore the data controller.

The Data Protection Rules require certain organisations to appoint a Data Protection Officer ("**DPO**") giving them prescribed responsibilities. The Data Protection Officer for the School is (TBD). The DPO will have overall responsibility for the School's compliance with the Data Protection Rules. The DPO's responsibilities will include, but are not limited to, the following tasks:

- Keeping the School's GB up to date with any changes to the way the school processes data;
- Taking steps to promote individuals' awareness of why the school needs their personal information, how the School will use it and with whom the School may share it;
- Setting out clear procedures for responding to requests for access to personal information, known as subject access requests;
- Arranging appropriate data protection training for school staff so they are aware of their responsibilities;
- Ensuring that staff are aware of this Policy and are following it; and
- Ensuring that new software or new services for the school are compliant, and that data protection impact assessments are carried out where necessary.

The School will ensure that the DPO is provided with resources and support to fulfil all of their responsibilities. Individuals may contact the DPO regarding any issues relating to the processing of their data by the School or the exercise of any of their rights in relation to it. Contact details for the DPO can be found at the end of this Policy, in the Contact Information section.

The DPO will be responsible within school for the following tasks:

- Ensuring that individuals are made aware of the Privacy Notice (see section 4) as and when any information is collected;
- Checking the quality and accuracy of the information held by the school;
- Applying the School's records retention schedule to ensure that information is not held longer than necessary by the school (the schedule can be found by visiting the School's intranet).
- Ensuring that when information is authorised for disposal, it is done so appropriately;
- Ensuring that appropriate security measures are in place to safeguard personal information, whether it is held in paper files or electronically;
- Only sharing personal information when it is necessary, legally appropriate to do so and in accordance with the Privacy Notice; and
- Ensuring that staff in the school are aware of this Policy and are following it.

The School will renew its registration with the Information Commissioner's Office (ICO) if and when necessary and pay any fees due to the ICO.

### 3.1 Responsibilities of Staff

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely;
- Personal information is not disclosed orally, in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party;
- Information or data about pupils is only shared with other staff as necessary and only by secure methods (such as the secure email provider). Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases; and
- Any additional associated policies are complied with (see section 9).

## 4. Privacy Notice

When any information is collected about individuals, they must be made aware of the Privacy Notices (see Appendix 1 and 2 for templates which should be adapted). The Privacy Notice provides information about what, why and how information is processed. You should make yourselves aware of the Privacy Notice, which should be read in line with this Policy.

## 5. Processing, Disclosure and Sharing of Information

The School processes personal data for a number of different purposes including:

| Lawful Ground for Processing  | Examples   |
|---|--|
| Where we have your consent  | Posting photographs of a pupil on the School's website<br>Providing pupil information for the administration of a school trip<br>Taking fingerprints for catering purposes               |
| Where it is necessary for the performance of a contract to which an individual is party | Providing information to a school photographer about photos required for a pupil   |
| Where it is necessary for compliance with a legal obligation                            | Passing on pupil information to the Department for Education<br>Passing on pupil information to the Local Authority  |
| Where it is necessary to protect the vital interests of an individual                   | Passing on information about a pupil's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that pupil or another individual |
| Where it is necessary for performance of a task in the public interest                  | Updating and maintaining a pupil's educational record as the pupil develops and progresses<br>Carrying out safeguarding activities   |

The School may also share data that they hold with members of staff, relevant parents/guardians, other schools within the LA, Local Authorities, the Department for Education, Ofsted, statutory bodies and other authorities where it is necessary to do so or where we are permitted to do so e.g. for the prevention of crime, to health professionals and examination bodies or any other body that the School or the school deems appropriate. Any sharing of data must be in accordance with the Data Protection Rules, this Policy and the Privacy Notice.

If the School receive enquiries from third parties, particularly by telephone, it is important to be careful about what data is disclosed. The following steps should be followed:

- Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the information they have requested;
- Require the third party to put their request in writing in order to verify their identity and their entitlement to the data requested;
- If in doubt, refer the request to the DPO of the School;
- When providing information to a third party, do so only in accordance with the Data Protection Rules, the Privacy Notice and this Policy; and
- Consider if a parent or guardian should have access to a pupil's information or whether the pupil is old enough to make any requests themselves.

### 5.1 Images and Biometric Data

- **Websites** – Where personal information, including images, is placed on the School's website, consent will be sought from the individual as appropriate.
- **Photographs** – Permission will be sought from the individual by the School before photographs of the individual are used or displayed, including in the school prospectus, newsletter or any other such publication where they can be clearly identified individually.
- **CCTV** – Where the school uses CCTV, it is responsible for ensuring procedures for use are in compliance with this Policy and with the CCTV Code of Conduct which can be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/>.
- **Fingerprints** – Where fingerprint records are taken from secondary pupils for catering or similar purposes, explicit consent will be sought from the individual as appropriate.
- **Social Media** – Where personal information, including images, is placed on the school's social media platforms e.g. Facebook/Twitter/LinkedIn, etc., consent will be sought from the individual as appropriate.

## 6. Requests for Access to Information

Any person whose personal information is held by the School has a right to ask for access to this information. These requests will be free-of-charge in almost all circumstances on and after 25 May 2018 (a £10 fee may be charged up to and including 24 May 2018). Any requests must be made in writing to the school's DPO. A response to any such request must be dealt with within one month from the date on which the request was received, if it is received on or after 25 May 2018 (or within 40 days if the request was made up to and including 24 May 2018).

Unlike the separate right of access to a pupil's progress and attainment record, the right to make a subject access request is the pupil's right. Parents/guardians are only entitled to access information about their child (by making a request) if the child is unable to act on their own behalf e.g. because the child is not mature enough to understand their rights or if the child has given their consent. If you are unsure about whether or not to provide information about a pupil to a parent or guardian, please speak to the DPO before providing any information.

Requests that fall under the Freedom of Information Act 2000 will be dealt with in accordance with the School's Freedom of Information Policy.

More information and detailed guidance can be found by visiting [www.ico.gov.uk](http://www.ico.gov.uk).

Individuals also have other legal rights under the Data Protection Rules, including to object to and prevent processing in certain circumstances and to have inaccurate personal data corrected or deleted. More information on these rights can be found in the Privacy Notice under "Requesting access to personal data".

## 7. Complaints and Breach Notification

Complaints should be made following the School's Complaints Procedure.

Information about how the School will deal with data breaches, including who staff should contact if they believe there may have been a data breach, can be found in the School's Data Breach Procedure (Appendix 3). The Data Protection Rules contain requirements about handling of breaches, which the School must comply with, so please ensure that you immediately report any breaches in accordance with the Data Breach Procedure.

## 8. Contact Information

The Data Protection Registration Number for Chamberlayne College for the Arts is Z123830XA copy of the registration can be found at <https://ico.org.uk/ESDWebPages/Entry/Z123830X>.

The School's DPO is Elaine Pearson, Business and Finance Manager, who can be contacted by email at [Elaine.pearson@chamberlayne.org](mailto:Elaine.pearson@chamberlayne.org), by telephone on [023 8044 7820](tel:02380447820) or at the school:

## 9. Associated Policies

- Freedom of Information Policy
- Complaints Procedure
- Acceptable Use of IT Policy



## **Appendix 1: Privacy Notice (Pupils)**

### **Privacy Notice (How we use pupil information)**

#### **Why do we collect and use pupil information?**

We collect and use pupil information on the following grounds:

- where you, the pupil (if aged 13 or over), or your parent or guardian (if under 13), have given consent to us doing so for a specific purpose;
- where it is necessary in order for the school to carry out its legal duties;
- where it is necessary when we agree a contract with an organisation and when you are involved (eg: school photographer or epraise);
- where it is necessary to protect your vital interests or those of another person;
- where it is necessary for the performance of a task carried out by the school in the public interest; and
- where it is necessary for recording purposes.

Special categories of data include those relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health; and
- sex life or sexual orientation.

Special categories of data can only be processed if the School also meets one of the following conditions:

- The individual has given explicit consent to the processing of it;
- The data is manifestly made public by the individual;
- The processing is necessary:
  - For carrying out and exercising the School's or the individual's rights for employment purposes or social security and social protection purposes as authorised by law;
  - To protect the vital interests of an individual who is physically or legally incapable of giving consent;
  - For the establishment, exercise or defence of legal claims;
  - For reasons of substantial public interest, on a legal basis that is proportionate to the aim pursued and provides for suitable and specific measures to safeguard the individual's rights;
  - For medical reasons including for medical diagnosis and provision of treatment; and
  - For reasons of public interest in the area of public health.

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to assess pupils;
- to provide appropriate pastoral care;
- to review pupil outcomes across the School;
- to carry out safeguarding activities;
- to provide services and assess the quality of our services; and
- to comply with the law regarding data sharing.

**The categories of pupil information that we collect, hold and share include:**

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, nationality, country of birth and language, including English as an additional language information);
- Eligibility information (such as for free school meals and pupil premium);
- Assessment information (such as results of examinations and mock examinations);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Medical information;
- Special Educational Needs information;
- Exclusions/behavioural information;
- Post-16 learning information; and
- Fingerprints for secondary age pupils for catering purposes.
- CCTV images and videos

**Collecting pupil information**

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

**Storing pupil data**

We hold pupil data for the period of time set out in the School's record retention schedule (details of which are available upon request); this may involve data being held until a pupil has reached the age of 25.

**Who do we share pupil information with?**

We routinely share pupil information with:

- schools that the pupil attends after leaving us;
- the relevant local authority;
- the Department for Education (DfE); and
- health and wellbeing professionals that provide pupil services for our school (such as speech and language therapists and educational psychologists).

We may also share data with third party suppliers who process data on our behalf, such as publishers of school handbooks, official photographs and web designers or IT providers.

**Aged 14+ qualifications**



For pupils enrolling for post-14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications.

### **Why we share pupil information**

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the DfE under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

### **Data collection requirements:**

To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

### **Youth support services**

#### **What is different about pupils aged 13+?**

Once our pupils reach the age of 13, we also pass pupil information to the local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services and careers advisers.

A parent/guardian can request that **only** their child's name, address and date of birth is passed to the local authority or provider of youth support services by informing us. This right is transferred to the child/pupil once he/she reaches the age of 16.

#### **Our pupils aged 16+**

We will also share certain information about pupils aged 16+ with the local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services and
- careers advisers.

For more information about services for young people, please visit the local authority's website.

### **The National Pupil Database (NPD)**

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the DfE, for the purpose of data collection, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The DfE may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;
- producing statistics; and
- providing information, advice or guidance.

The DfE has robust processes in place to ensure that the confidentiality of our data is maintained and there are stringent controls in place regarding access to and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and are based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>.

For information about which organisations the DfE has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>.

To contact the DfE: <https://www.gov.uk/contact-dfe>.

### **Who may provide us with data about you**

We receive information about pupils from a number of external sources, e.g. previous schools, local authorities, social services and the police.

We will explain to you when we receive information from any of these sources.

## Requesting access to your personal data

Under data protection legislation, parents and pupils have certain rights to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's progress and attainment record, contact the school's Data Protection Officer.

Please note that parents/guardians do not have an automatic right to see all information about their child and certain rights may only be exercised by a pupil or with their permission.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the data protection regulation.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

### Contact:

If you would like to discuss anything in this privacy notice, obtain a copy of your personal data or exercise any of your rights, please contact:

- The School's Data Protection Officer, Elaine Pearson, Business and Finance Manager, who can be contacted by email at [Elaine.pearson@chamberlayne.org](mailto:Elaine.pearson@chamberlayne.org) or by telephone on 023 8044 7820.



## Appendix 2: Privacy Notice (Staff)

### Introduction

- 1 This notice is to help you understand **how** and **why** we collect personal information about you and **what** we do with that information. It also explains the decisions that you can make about your own information.
- 2 The School is ultimately responsible for how we handle your personal information. In this privacy notice, we use the term "School" to mean both the School and the GB.
- 3 If you have any questions about this notice, please contact the Data Protection Officer (DPO).
- 4 This notice is aimed at all School staff (including Governors, volunteers and certain contractors) and applicants for employment vacancies. This privacy notice does not form part of your contract of employment and the School may amend this notice at any time.

### What is personal information?

- 5 Personal information is information which is about you and from which you can be identified.
- 6 This includes your contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

### What personal information does the School hold about you and how is this obtained?

- 7 We set out below examples of the personal information the School holds about you and where this personal information comes from.
- 8 Information about you is gathered during the recruitment process:
  - 8.1 such as information about your education, qualifications and professional achievements;
  - 8.2 you will provide certain information to us, for example, on your application form and during any interviews;
  - 8.3 we may obtain information from publicly available sources such as your social media profiles; and
  - 8.4 we will receive your personal information (from you and third parties) when we carry out pre-employment checks, for example, when we receive references, confirmation of your fitness to work, your right to work in the UK and criminal records checks.
- 9 We will hold information about your job performance. This includes information about skills, achievements, career progression, performance and disciplinary related matters.
- 10 We hold and use your financial information, such as, your bank details, your salary and pension details.
- 11 We will hold information about any physical or mental health condition you may have which is disclosed to the School during the recruitment process or at any stage during your employment.

- 12 We will hold information about any protected characteristics you may have (e.g. a disability) which you provide, for example on the Equal Opportunities Monitoring Form.
- 13 Your personal information may be created internally by the School during the course of your employment. An email from the Head to a member of staff complimenting them on GCSE results would be an example of this.
- 14 Your personal information may be acquired from outside of the School community such as from occupational health practitioners or from public authorities such as the Police or the Local Authority Designated Officer.
- 15 Pupils may provide us with your personal information, for example, if a pupil emails their tutor to say how much you are helping them with their work.

### **Why does the School use your personal information?**

- 16 We commonly use personal information for:
  - 16.1 ensuring that we provide a safe and secure work environment;
  - 16.2 providing employment services (such as payroll and references);
  - 16.3 providing training and support;
  - 16.4 protecting and promoting the School's interests and objectives (including fundraising);
  - 16.5 personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer. For example, to pay staff and to monitor their performance;
  - 16.6 safeguarding and promoting the welfare of all staff and pupils; and
  - 16.7 fulfilling our contractual and other legal obligations.
- 17 Some specific examples of when the School uses your personal information as set out below:
  - 17.1 We use your personal information to consider your suitability to work in your role at the School.
  - 17.2 We will check that you have the right to work in the UK by reviewing your identification documents and keeping copies on your personnel file.
  - 17.3 We may use your personal information in addressing performance or disciplinary concerns.
  - 17.4 We will use information relating to any medical condition you may have in order to verify fitness to work, monitor sickness absence and comply with our duty of care towards you.
  - 17.5 We may use your information when dealing with complaints and grievances (e.g. from other staff and parents).
  - 17.6 We may use information about you and photographs and video recordings of you for marketing and promotion purposes including School publications, in social media and on the school website.

- 17.7 We may use your information to enable the development of a comprehensive picture of the workforce and how it is deployed.
- 17.8 We may use your information to inform the development of recruitment and retention policies.
- 17.9 We may also allow external publication of certain media where appropriate (for example, a photograph or article in a local newspaper).
- 17.10 We may also make recordings for teaching purposes, for example, recording a drama lesson to provide feedback to you or pupils. We may also record lessons for pupils who were not able to attend in person.
- 17.11 We use CCTV recordings for the purposes of crime prevention and investigation and also in connection with our obligation to safeguard the welfare of pupils, staff and visitors to the School site.
- 17.12 The School regularly monitors and accesses its' IT system for purposes connected with the operation of the School. The IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School may also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).
- 17.13 The purposes of such monitoring and accessing include:
  - 17.13.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and
  - 17.13.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.
- 17.14 Monitoring may be carried out on a random basis or it may be carried out in response to a specific incident or concern.
- 17.15 The School also uses software which automatically monitors the IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).
- 17.16 The monitoring is carried out by the School. If anything of concern is revealed as a result of such monitoring, then this information may be shared with the Headteacher / Line Manager this may result in disciplinary action. In exceptional circumstances concerns may need to be referred to external agencies such as the Police.

### **How does the School share staff personal information with third parties?**

- 18 We may need to share your information with the Disclosure and Barring Service (**DBS**) or the National College for Teaching and Leadership (**NCTL**) when carrying out safer recruitment checks or in making a referral to the DBS or the NCTL.

- 19 We may need to share your information with UK Visas and Immigration (**UKVI**) in order to sponsor you as an employee if you are from outside of the European Economic Area and to meet the School's sponsorship duties.
- 20 Occasionally we may use consultants, experts and other advisors (including legal advisors) to assist us in fulfilling our obligations and to help run the School properly. We might need to share your information with them if this is relevant to the work they carry out.
- 21 In accordance with our legal obligations, we may share information with Ofsted, for example, during the course of an inspection, and may need to share your information with the Department for Education.
- 22 We may share information about you with the other schools in the LA. For example, information about which pupils you teach and/or information relating to the pre-employment checks the School has carried out.
- 23 We may share some of your information with our insurance company or benefits providers, for example, where there is a serious incident.
- 24 If the School is dealing with a complaint or grievance (e.g. from a parent) we may share your information with other parties, for example, the appropriate staff at the School, the parents making the complaint and governors.
- 25 We may share your information with individuals connected to the School who are exercising their data protection rights, for example, when responding to a subject access request.
- 26 We may share personal information about staff with the relevant statutory agencies who may need this information to investigate allegations of misconduct.
- 27 We may need to share your information with the police for the prevention and investigation of crime and the prosecution of offenders.
- 28 CCTV recordings may be disclosed to third parties such as the police.
- 29 We may share your information with parents and pupils where this is related to your professional duties.
- 30 We may need to share your information if there is an emergency, for example, if you are hurt in an accident.
- 31 We sometimes use contractors to handle personal information on our behalf. The following are examples:
  - 31.1 Payroll provider;
  - 31.2 CPOMs
  - 31.3 SIMS

**For how long does the School keep staff personal information?**

- 32 We keep your information for as long as we need to in relation to your employment. We will keep some information after you have left the School in case this is needed, for example, in relation to our legal obligations and in accordance with the School record retention schedule.

- 33 In exceptional circumstances we may keep your information for a longer time than usual but we would only do so if we had a good reason and only if we are allowed to do so under data protection law.
- 34 We can keep information about you for a very long time or even indefinitely if we need this for historical, research or statistical purposes. For example, if we consider the information might be useful if someone wanted to write a book about the School.

The school have a records retention schedule which can be found on the shared area under POLICIES or by requesting a copy from the Data Protection Officer.

### **Processing in line with your rights**

- 35 From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights. Your rights are as follows:
- 35.1 if information is incorrect you can ask us to correct it;
  - 35.2 you can also ask what information we hold about you and be provided with a copy. We will also give you extra information, such as why we use this information about you, where it came from and what types of people we have sent it to;
  - 35.3 you can ask us to delete the information that we hold about you in certain circumstances. For example, where we no longer need the information;
  - 35.4 you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer;
  - 35.5 our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy.

You also have the right to:

- 35.6 object to processing of personal data that is likely to cause, or is causing, damage or distress
- 35.7 prevent processing for the purpose of direct marketing
- 35.8 object to decisions being taken by automated means
- 35.9 in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 35.10 claim compensation for damaged caused by a breach of the Data Protection regulations

The DPO can give you more information about your data protection rights.

### **Our legal grounds for using your information**

This section contains information about the legal basis that we are relying on when handling your information as described above.

#### Contractual obligation

We will need to use your information in order to comply with our contractual obligations. For example:

- we need your name and bank details so that we can pay you your salary;
- we may need to provide your personal information to a pension provider;
- we also need to use your personal information to provide contractual benefits;
- if we provide you with accommodation under your contract we will use your personal information as part of this provision.

#### Legal obligation

We have to comply with various laws and this entitles us to use your information where necessary. For example:

- we have to make sure that you have the right to work in the UK;
- to fulfil our duty of care to you and your colleagues;
- we have to fulfil our safeguarding duties towards pupils; and
- we may be legally obliged to disclose your information to third parties such as the DBS, local authorities or the police.

#### Vital interests

We may use your information where this is necessary to protect your vital interests or someone else's. For example, to prevent someone from being seriously harmed or killed.

#### Performance of a task carried out in the public interest

We use your information for a variety of reasons in the public interest, for example:

- facilitating our teaching requirements, for example, to help us decide which member of staff will teach a particular class based on skills, experience, qualifications and so on;
- looking after your welfare and development and the welfare and development of others;
- safeguarding and promoting the welfare of our pupils;
- ensuring the security of the school site which may involve issuing you with a photocard;
- making sure that you are complying with your employment obligations;
- facilitating the efficient operation of the School; and
- ensuring that we comply with all of our legal obligations.

If you object to us using your information when we are relying on this ground please speak to the DPO.

The School must also comply with an additional condition where it processes special categories of personal information. These special categories are as follows: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic

information, biometric information, health information, and information about sex life or orientation. The grounds that we are relying on to process special categories of personal data are set out below:

Employment, social security and social protection

The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the School and staff in the field of employment, social security or social protection.

Vital interests:

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal claims:

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical purposes

This includes medical treatment and the management of healthcare services.

Substantial public interest

The School is also allowed to use special categories of personal information where doing so is necessary in the substantial public interest. This is similar to "Public interest" in the table above, for example the School may use special categories of information when providing an education to pupils, looking after the welfare of pupils or when the School is inspected.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid. Please speak to the DPO if you would like to withdraw any consent given.

In some cases, we will rely on more than one of the grounds above for a particular use of your information. For example, we may rely on legitimate interests and public interest grounds when using your information to safeguard our pupils.

### Further information

- 36 **Contact:** If you would like any further information about anything within this notice please contact the Data Protection Officer, Elaine Pearson
- 37 Please speak to the Data Protection Officer in your school, if:
  - 37.1 you object to us using your information for marketing purposes e.g. to send you information about school events; or

- 37.2 you would like us to update the information we hold about you; or
- 37.3 you would prefer that certain information is kept confidential.
- 38 **ICO:** If you consider that we have not acted properly when using your personal information you can contact the Information Commissioner's Office: [ico.org.uk](http://ico.org.uk).
- 39 **If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance.**

### Appendix 3: Pupil Photograph & Video Consent Form

#### PUPIL DIGITAL PHOTOGRAPHS AND/OR VIDEOS CONSENT FORM

Occasionally, we may take photographs of the pupils at our School. We may use these images in our schools' prospectus, other printed publications, websites, social media platforms (e.g. Facebook, Twitter, etc.) and/or on display boards.

We may also take videos for educational use and/or use as evidence for Ofsted. These videos may potentially also be used in websites, social media platforms and display screens.

We may also send the images to the news media (or they may come into the school and take pictures/videos), who may use them in printed publications and on their website, and store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, or on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

**Terms of Use**

- We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers, or for any consequences arising from publication.
- We will not use the personal details of a Pupil, including their full name, alongside a photographic image on our website, in our school prospectus or in any other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has been awarded a Headteacher Commendation.
- If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason.
- We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
- We may use group or class photographs or footage with very general labels e.g. 'maths lesson'.

**Consent**

|   |          |
|---|----------|
| I give permission for my child's image to appear in the school prospectus and/or other printed publications that the school produce for promotional purposes.   | YES / NO |
| I give permission to the school to use my child's image on school/School websites.  | YES / NO |
| I give permission to the school to use images of my child in notifications via social media (to include Twitter/Facebook) to share details of school events and activities.   | YES / NO |
| I give permission for you to record my child's image on video or webcam to be displayed online via school or other websites.  | YES / NO |
| I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images/footage the media may take themselves if invited to the school to cover an event. | YES / NO |

**I have read and understood the above information.**



|              |                   |
|--------------|-------------------|
| Pupil Name:  | Year Group        |
| Parent Name: | Parent Signature: |
| Date:        |                   |

#### **Appendix 4: Staff Photograph & Video Consent Form**

##### **STAFF DIGITAL PHOTOGRAPHS AND/OR VIDEOS CONSENT FORM**

Occasionally, we may take photographs of staff at our School. We may use these images in our school's prospectuses, other printed publications, websites, social media platforms (e.g. Facebook, Twitter, etc.) and/or on display boards.

We may also take videos for educational use and/or use as evidence for Ofsted. These videos may potentially also be used in websites, social media platforms and display screens.

We may also send the images to the news media (or they may come into the school and take pictures/videos), who may use them in printed publications and on their website, and store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, or on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

**Terms of Use**

- We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers, or for any consequences arising from publication.
- We will make every effort to ensure that we do not allow images to be taken of any staff for whom we do not have permission or who are ‘at risk’ or disallowed from having their photographs taken for legal or social reasons.
- We may use group or class photographs or footage with very general labels e.g. ‘maths lesson’.

**Consent**

|   |          |
|---|----------|
| I give permission for my image to appear in the school prospectus and/or other printed publications that the school produce for promotional purposes.   | YES / NO |
| I give permission to the school to use my image on school/School websites.  | YES / NO |
| I give permission to the school to use images of me in notifications via social media (to include Twitter/Facebook) to share details of school events and activities.   | YES / NO |
| I give permission for you to record my image on video or webcam to be displayed online via school or other websites.  | YES / NO |
| I give permission for images of me to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images/footage the media may take themselves if invited to the school to cover an event. | YES / NO |

**I have read and understood the above information.**

|             |                  |
|-------------|------------------|
| Staff Name: | Staff Signature: |
| Date:       |                  |



## Appendix 5: Data Breach Procedure for Chamberlayne College for the Arts (the "School")

### 1. About this procedure

This procedure describes the actions that must be taken by staff to report any incident which may result in a personal data breach. A "personal data breach" is defined in Article 4(12) of the General Data Protection Regulation as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a personal data breach. The term "incident" is used in this policy to describe any situation which may, upon investigation, turn out to be a personal data breach.

This policy should be read in conjunction with the Data Protection Policy which can be found on the School's website.

### 2. Identifying an incident

An incident may come to light in a number of ways. For example, it could occur by:

- direct observation e.g. where a member of staff spots that personal data has been sent to the wrong email address;
- being reported to us by a pupil or parent: e.g. where a pupil notifies us that she/he has received personal data relating to another pupil;
- being reported to us by another party, such as a contractor, a local authority or a member of the public; or
- an audit / review revealing that an incident had occurred.

### 3. Actions to take once an incident has been identified

Whenever an incident is identified, the following actions must be taken:

|    | Action  | Responsibility   | Timelines   |
|----|---|--|---|
| 1. | Report the incident to the Data Protection Officer of the School                | Member of staff who was first made aware of the incident | <b>Immediately after the incident is identified</b> |
| 2. | Investigate and identify the full details of the incident to identify the cause | Data Protection Officer (with the assistance of the      | <b>As soon as possible following the incident</b>   |

|    |   |  |  |
|----|---|--|--|
|    |   | colleague who reported the incident)   | <b>being reported</b>  |
| 3. | Identify any remedial action (see section 4, below). Inform Headteacher.  | Data Protection Officer for the school | <b>As soon as possible following the incident being reported</b>                 |
| 4. | Complete a formal Personal Data Breach Form and return it to the School's Data Protection Officer   | Person reporting the data breach       | <b>Within 48 hours of the incident being identified</b>                          |
| 5. | Review the Personal Data Breach Form and determine whether the incident constitutes a personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach) | Data Protection Officer                | <b>As soon as possible following step 4</b>                                      |
| 6. | If necessary, decide whether to notify (i) the ICO; and/or (ii) individual data subjects, of the personal data breach (see section 5, below)  | Data Protection Officer                | <b>As soon as possible following step 4</b>                                      |
| 7. | If necessary, notify the ICO of the personal data breach  | Data Protection Officer                | <b>Within 72 hours of the incident being identified</b>                          |
| 8. | If necessary, notify individual data subjects of the personal data breach   | Data Protection Officer                | <b>Without undue delay (in practice this should be done as soon as possible)</b> |

#### 4. Taking remedial action

Following the reporting of the issue, the School's Data Protection Officer shall take remedial action, in particular where pupils or parents are affected in any way by the personal data breach. Pupils or parents may suffer distress and inconvenience where they are aware that a breach has occurred. In some cases, they may be at risk of suffering financial detriment or physical harm as a result of the breach.

Remedial action should seek to mitigate any risks the pupil or parent has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the School's reputation. Action will be dependent on case specifics, but the Data Protection Officer should consider the School's responsibility to act in the best interests of pupils and parents.

Remedial action might include the following:

- If personal data is in the hands of a third party, it should be retrieved from the third party or deleted from the third party's IT system (please speak to IT for assistance);
- If the breach arose as a result of an IT issue, the source of the issue should be identified and rectified (please speak to IT for assistance);
- If the breach arose as a result of human error, the individual should be made aware of the error and where appropriate asked to undertake additional training or (only in the most serious cases) be subjected to disciplinary action.

## **5. Notifying a personal data breach**

Under the General Data Protection Regulation, there is an obligation to report a personal data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of us becoming aware of the breach.

There is an exception to this reporting requirement where the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the School's Data Protection Officer following receipt of the Personal Data Breach Form.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A personal data breach that may result in a high risk to individuals may include where a parent is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then the School's Data Protection Officer must inform them of the breach by letter and make a formal apology. The School's Data Protection Officer will make the final decision as to whether notifying individuals is required.

Where pupils or parents are aware that they are the subject of a personal data breach, then they must be issued with a written apology. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

Where appropriate, remedial action should also consider anyone other than the pupil(s) or parent(s) who may also have been affected indirectly. These individuals should also be sent a written apology to minimise the School's reputational damage.

As well as the requirement to report personal data breaches to the ICO, it may also be necessary to report them to other authorities such as the police. These actions should only be undertaken following consultation with the School's Data Protection Officer.

## **6. Follow-up action**

To ensure that we learn from our mistakes, the school responsible is required not only to confirm that remedial action has taken place, but also that the causes of the personal data breach have been analysed

and action taken to ensure similar breaches do not occur again. Confirmation of this action is reported and saved by the School's Data Protection Officer as an audit trail.

## **7. Central logging of the issue**

Once the school responsible has confirmed remedial action and any appropriate follow-up action, then, subject to:

- the pupil(s) or parent(s) being satisfied with the remedial action taken in respect of the breach and;
- the Data Protection Officer being satisfied that regulatory procedures have been followed,

then the breach can be marked as closed by the Data Protection Officer.

A copy of all breach forms will be kept by the Data Protection Officer and stored securely.

## Appendix 6: Personal Data Incident Reporting Form

Please complete this form with as much detail as possible and email it to the School's Data Protection Officer at [elaine.pearson@chamberlayne.org](mailto:elaine.pearson@chamberlayne.org). If you do not have sufficient information to complete all of the form, please complete everything you can and return it to the DPO as soon as possible and no later than 48 hours after you or the member of staff in your school became aware of the incident.

| <b>Part 1: Summary (TO BE COMPLETED BY THE PERSON REPORTING THE BREACH)</b>                                    |  |
|--|--|
| Name and department of person reporting:   |  |
| Date of report:  | <i>[Please state the date you are completing the form]</i>   |
| Time and date incident first identified by the school/staff member:  |  |
| Time and date incident occurred (if different):  |  |
| Circumstances of the incident:   | <i>[Please give a summary of what actually happened]</i>   |
| <b>Part 2: Details of the personal data incident (TO BE COMPLETED BY THE PERSON REPORTING THE DATA BREACH)</b> |  |
| Nature of the incident:  | <i>[e.g. which rules/procedures were breached and how did it happen? If you are not sure of the rules, just explain which internal procedure was not followed or ask the DPO for assistance]</i> |
| Categories of data subject affected:   | <i>[e.g. pupils, parents, employee, others]</i>  |

|   |  |
|---|--|
| Approximate number of data subjects affected (if known):  |  |
| Possible consequences of the incident for data subjects:  | <i>[State if there is likely to be any detriment to individuals. If yes, please provide details]</i> |
| <b>Part 3: Actions taken in response to the incident (TO BE COMPLETED BY THE DATA PROTECTION OFFICER)</b> |  |
| What mitigating action was taken or will be taken in response to the incident?                            |  |
| Follow up action taken to prevent similar future breaches   |  |
| <b>Part 4: DPO actions (TO BE COMPLETED BY THE DATA PROTECTION OFFICER)</b>                               |  |
| Does the incident constitute a near miss or a personal data breach?                                       |  |
| If it is a personal data breach, is it notifiable to the ICO:   | Y / N<br>If Y, date notified<br>If N, reason for not notifying the breach                            |
| If it is a personal data breach, is it notifiable to data subjects:                                       | Y / N<br>If Y, date notified<br>If N, reason for not notifying the breach                            |
| Date issue closed:  |  |



CHAMBERLAYNE COLLEGE FOR THE ARTS  
Expect More. Achieve More.

