**DATA PROTECTION:**

**RECORDS MANAGEMENT & RETENTION**



| POLICY WRITTEN BY:  | PROPRIETORS  |
| --- | --- |
| DATE POLICY PREPARED/REVIEWED: | November 2022, August 2023, |
| DATE FOR NEXT REVIEW:  | August 2025 |

ARTS EDUCATION is required to keep certain personal data about its staff and students in order to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Our school aims to ensure that all personal data collected about staff, students, parents, Governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation 2018](http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf) (GDPR) and the provisions as set out in the UK Data Protection Act (DPA) 2018.

ARTS recognises the importance of good quality file keeping and records management and views this as a fundamental part of its work.

Consequently, we have a responsibility to ensure that all records are:

* Stored in the most effective way
* Kept as securely as possible
* Easily traced and retrievable
* Retained for only as long as necessary
* Disposed of appropriately

All staff have been provided with Data Protection and GDPR awareness training and will receive annual refresher training alongside any training/information updates as and when deemed appropriate to ensure the ongoing best practice in data protection in the school. Any breach of this policy will be taken seriously and may result in formal action being taken.

**Definitions**

**What is a record?**

A record is defined as ‘recorded information, in any form, created or received and maintained by ARTS in the transaction of its business or conduct of affairs and kept as evidence of such activity.’

**A record** should be regarded as information in its final form, and not subject to alteration

**What is a document?**

A document is an object that may still be subject to alteration by editing.

A document may ultimately become a record.

| **Term** | **Definition** |
| --- | --- |
| Personal data | Any information relating to an identified, or identifiable, living individual. This may include the individual’s: * Name (including initials)
* Identification number
* Location data
* Online identifier, such as a username

It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.  |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual’s: * Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Genetics
* Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
* Health – physical or mental
* Sexual orientation
 |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed.  |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| Data processor  | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data |

 ARTS processes personal data relating to parents, students, staff, Governors, visitors and others, and is, therefore, a data controller. As a data controller, the school is legally required to register with the Information Commissioner’s Office (ICO) annually under the GDPR. ARTS School is registered with the ICO under reference **ZB394234**.

**Collecting Personal Data**

 Lawfulness, fairness and transparency

We will only process personal data where we have one of six ‘lawful bases’ (legal reasons) to do so under data protection law:

* The data needs to be processed so that the school can fulfil a contract with the data subject, or the data subject has asked the school to take specific steps before entering into a contract.
* The data needs to be processed so that the school can comply with a legal obligation.
* The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life.
* The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions.
* The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party (provided the individual’s rights and freedoms are not overridden).
* The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

* The individual (or their parent/carer when appropriate in the case of a student) has given explicit consent.
* The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
* The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
* The data has already been made manifestly public by the individual.
* The data needs to be processed for the establishment, exercise or defence of legal claims.
* The data needs to be processed for reasons of substantial public interest as defined in legislation.
* The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under the law.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

* The individual (or their parent/carer when appropriate in the case of a student) has given consent.
* The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
* The data has already been made manifestly public by the individual.
* The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
* The data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

**Limitation, minimisation and accuracy**

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted, destroyed or anonymised. This will be done in accordance with the school’s Record Retention Schedule.

**Sharing Personal Data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

* There is an issue with a student or parent/carer that puts the safety of our staff at risk
* We need to liaise with other agencies – we will seek consent as necessary before doing this
* Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, educational support services. When doing this, we will:
	+ only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
	+ establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
	+ only share data that the supplier or contractor needs to carry out their service.
* We will also share personal data with law enforcement and government bodies where we are legally required to do so.
* We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

 **Subject Access Requests**

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:

* Confirmation that their personal data is being processed.
* Access to a copy of the data.
* The purposes of the data processing.
* The categories of personal data concerned.
* Who the data has been, or will be, shared with.
* How long the data will be stored for, or if this is not possible, the criteria used to determine this period.
* Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
* The right to lodge a complaint with the ICO or another supervisory authority.
* The source of the data, if not the individual.
* Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
* The safeguards provided if the data is being transferred internationally.

Subject access requests must be submitted in any form to the DPL but we may be able to respond to requests more quickly if they are made in writing and include:

* Name of individual making the request.
* Correspondence address.
* Contact telephone number and email address.
* Details of the information requested.

If an employee receives a subject access request they must immediately forward it to the school’s Data Protection Lead.

**Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student’s ability to understand their rights will always be judged on a case-by-case basis.

**Responding to subject access requests**

When responding to requests, we:

* Will ask the individual making the request to provide two forms of identification.
* Will contact the individual via phone to confirm the request was made.
* Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
* Will provide the information free of charge.
* May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

* Might cause serious harm to the physical or mental health of the student or another individual.
* Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child’s best interests.
* Would include another individual’s personal data that we cannot reasonably anonymise, and we do not have the other individual’s consent and it would be unreasonable to proceed without it.
* Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or examination scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell him/her that he/she has the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

**Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

* Withdraw their consent to processing at any time.
* Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
* Prevent use of their personal data for direct marketing.
* Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
* Challenge decisions based solely on automated decision making or profiling (ie making or evaluating things about an individual based on their personal data with no human involvement).
* Be notified of a data breach in certain circumstances.
* Make a complaint to the ICO.
* Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the school’s Data Protection Lead.

**Parental Requests to See the Educational Record**

Parents, or those with parental responsibility, have a legal right to free access to their child’s educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing examination marks before they are officially announced.

**CCTV**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO’s code of practice for the use of CCTV.

We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Head and Site Manager.

**Photographs and Videos**

As part of our school activities, we may take photographs and record images of individuals within our school.

Where we need parental consent, we will clearly explain to both the parent/carer and student how the photograph and/or video will be used. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

* Within school on notice boards and in school magazines, brochures, newsletters, etc.
* Outside of school by external agencies such as the school photographer, newspapers, campaigns.
* Online on our school website or social media pages.

Where consent is required we will obtain written consent from parents/carers upon admission in Year 7 (or at the point of admission in other years).

Consent can be refused or withdrawn at any time by confirming this in writing to the Data Protection Lead. If consent is withdrawn, we will take all reasonable measures to delete all known photographs or videos.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

**Data Protection by Design and Default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

* Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
* Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
* Completing privacy impact assessments where the school’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
* Integrating data protection into internal documents, including this policy, any related policies and privacy notices.
* Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
* Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
* Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply. Maintaining records of our processing activities, including:
	+ For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
	+ For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

**Data Security**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

* Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
* Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
* Where personal information needs to be taken off site, staff must obtain prior approval from a member of the Senior Leadership Team and take full responsibility for the protection and security of that data whilst off site.
* Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals and should not use passwords from other sites.
* Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
* Staff, students or Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
* Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

**Disposal of Records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

**Personal Data Breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. All data breaches will be recorded on our internal data breach recording system system and shared with our DPO who will advise on further reporting required to the ICO. Where appropriate we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

* A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the Pupil Premium.
* Safeguarding information being made available to an unauthorised person.
* The theft of a school laptop containing non-encrypted personal data about students.

**Training**

All staff and Governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school’s processes make it necessary.

**Monitoring arrangements**

This policy will be reviewed annually by the school and presented to the Governing Body every two years for review and approval.

**Destruction of records table**

| Accident records  | 15 years  |
| --- | --- |
| Admission registers  | Permanent  |
| Children’s individual files  | 25 years or if died prior to age 18, 15 years from death  |
| Complaints  | 25 years  |
| Diaries  |  Keep the previous year |
| Electrical testing |  3 years  |
| Finance records |  6 years and then arrangements made for the secure destruction |
| Fire records |  3 years  |
| General correspondence  | Keep the previous year  |
| Incidents, events or occurrences that require notification to Ofsted  | 15 years |
| Inspection reports  | 3 years  |
| Insurance policies  | Permanent  |
| Lease arrangements  | Permanent  |
| Local operational policies and procedures  | Keep current version and previous version for 3 years  |
| Log books  | 3 years  |
| Medication records  | 25 years – should be archived with childcare file |
| Personnel records for ex-members of staff | 7 years and then securely destroyed |
| Staff Sign-in Books  | Current year plus previous year  |
| Team meetings  | 3 years |
| Visitor’s book  | 15 years |
| Young person’s meetings  | 15 years |
| Finance/accounts records (other than): |  Current year plus previous 6 years  |
| o Bank statements  | Current year plus previous 6 years  |
| o Cheque requisitions  | Current year plus previous 6 years  |
|  o Payroll  | Keep current year and previous year and destroy remainder |
| o Paid invoices  | Current year plus previous 6 years |