Data Protection Policy for Staff

The Arts Educational Schools

May 2018

1 Introduction

1.1 Data protection is an important legal compliance issue for The Arts Educational Schools (ArtsEd). On 25 May 2018, the General Data Protection Regulation (GDPR) was implemented. This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of pupils and students is at all times handled responsibly and securely.

1.2 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the School uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data - such as the right to access the Personal Data that the School holds on them.

1.3 As a school, we will collect, store and process Personal Data about our staff, pupils, students, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the School and will ensure that the School operates successfully.

1.4 You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.5 References to pupil apply to any person enrolled at The Arts Educational Schools independent school or sixth form and references to student apply to any person enrolled in further education or higher education or ArtsEd Extra at The Arts Educational Schools.

2 Data Protection Lead

The School has appointed Kathy-Ann Darmody (the Finance Director) as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

3 Key data protection terms used in this data protection policy are:

- Data controller – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' and students' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.

- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- Personal information (or personal data): any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions

of opinion about the individual or any indication of someone's intentions towards that individual.

- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

4 Application

4.1 This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, Trustees, contractors, agency and peripatetic staff, work experience / placement students and volunteers.

4.2 This policy does not form part of your contract of employment and may be amended by the School at any time.

5 The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

5.1 Processed **lawfully, fairly** and in a **transparent** manner;

5.2 Collected for **specific and explicit purposes** and only for the purposes it was collected for;

5.3 **Relevant** and **limited** to what is necessary for the purposes it is processed;

5.4 **Accurate** and kept **up to date**;

5.5 **Kept for no longer than is necessary** for the purposes for which it is processed; and

5.6 Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;

- documenting significant decisions and assessments about how we use personal data; and

- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

6 Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Policy, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff, parents or students;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7 What information falls within the scope of this policy

7.1 Data protection concerns information about individuals.

7.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

7.3 Information as simple as someone's name and address is their Personal Data.

7.4 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

7.5 Examples of places where Personal Data might be found are on a computer database; in a file, such as a pupil report; a register or contract of employment; pupils' exercise books, coursework and mark books; health records and email correspondence.

7.6 Examples of documents where Personal Data might be found are

7.6.1 a report about a child protection incident;

7.6.2 a record about disciplinary action taken against a member of staff;

7.6.3 photographs or recordings of pupils;

7.6.4 a tape recording of a job interview;

7.6.5 a recording of a performance;

7.6.6 contact details and other personal information held about pupils, students, parents and staff and their families;

7.6.7 contact details of a member of the public who is enquiring about a place at the School;

7.6.8 financial records of a parent, student or pupil;

7.6.9 information on a pupil's or student's performance; and

7.6.10 an opinion about a parent, pupil, student or colleague in an email.

7.7 These are just examples - there may be many other things that you use and create that would be considered Personal Data.

7.8 You must be particularly careful when dealing with Personal Data which falls into any of the categories below:

7.8.1 information concerning child protection matters;

7.8.2 information about serious or confidential medical conditions and information about special educational needs;

7.8.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

7.8.4 financial information (for example about parents, pupils, students and staff);

7.8.5 information about an individual's racial or ethnic origin;

7.8.6 political opinions;

7.8.7 religious beliefs or other beliefs of a similar nature;

7.8.8 trade union membership;

7.8.9 physical or mental health or condition;

7.8.10 sexual life;

7.8.11 genetic information;

7.8.12 information relating to actual or alleged criminal activity; and

7.8.13 biometric information (e.g. a pupil's or student's fingerprints following a criminal investigation).

7.9 These categories are referred to as **Critical School Personal Data** in this policy and in the information security policy. If you have any questions about your processing of these categories of Personal Data please speak to the Finance Director.

8 Your obligations

8.1 Personal Data must be processed fairly, lawfully and transparently

8.1.1 What does this mean in practice?

(a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

(b) People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is often provided in a document known as a privacy notice. Copies of the School's privacy notices can be obtained from the Finance Director or accessed on the School's website. You must familiarise yourself with the School's privacy notices.

(c) If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Finance Director.

(d) You must only process Personal Data for the following purposes:

(i) ensuring that the School provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education and learning for our pupils and students;

(iv) providing additional activities for pupils, students and parents (for example activity clubs);

(v) protecting and promoting the School's interests and objectives (for example fundraising);

(vi) safeguarding and promoting the welfare of our pupils and students; and

(vii) to fulfil the School's contractual and other legal obligations.

(e) If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Finance Director. This is to make sure that the School has a lawful reason for using the Personal Data.

(f) We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Finance Director if you think that you may need to obtain consent.

8.2 **You must only process Personal Data for limited purposes and in an appropriate way.**

8.2.1 What does this mean in practice?

(a) For example, if pupils or students are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in the School's prospectus).

8.3 **Personal Data held must be adequate and relevant for the purpose**

8.3.1 What does this mean in practice?

(a) This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil or student.

8.4 **You must not hold excessive or unnecessary Personal Data**

8.4.1 What does this mean in practice?

(a) Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's siblings if that Personal Data has some relevance, such as allowing the School to determine if a sibling fee discount is applicable.

8.5 **The Personal Data that you hold must be accurate**

8.5.1 What does this mean in practice?

(a) You must ensure that Personal Data is complete and kept up to date. For example, if a pupil, student or a parent notifies you that their contact details have changed, you should update the School's information management system.

8.6 **You must not keep Personal Data longer than necessary**

8.6.1 What does this this mean in practice?

(a) The School has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

(b) Please speak to the Finance Director for guidance on the retention periods and secure deletion.

8.7 **You must keep Personal Data secure**

8.7.1 You must comply with the following School policies and guidance relating to the handling of Personal Data:

(a) information security policy;

(b) policy on the use of photographs and videos of pupils or students;

(c) IT acceptable use policy for staff; and

(d) information and records retention policy.

8.8 **You must not transfer Personal Data outside the EEA without adequate protection**

8.8.1 What does this mean in practice?

(a) If you need to transfer personal data outside the EEA please contact the Finance Director. For example, if you are arranging a school trip to a country outside the EEA.

9 Processing of Credit Card Data

ArtsEd complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Finance Director.

10 Sharing Personal Data outside the School - dos and don'ts

10.1 Please review the following dos and don'ts:

10.1.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of the School - if in doubt - always ask your Manager.

10.1.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 7.8 above. For example, encryption should be used when sending details of a safeguarding incident to social services, or information to the pension provider.

10.1.3 **DO** make sure that you have permission from your Manager or the Finance Director to share Personal Data on the School website.

10.1.4 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the Finance Director where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

10.1.5 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

10.1.6 **DO NOT** disclose Personal Data to the Police without permission from the Finance Director (unless it is an emergency).

10.1.7 **DO NOT** disclose Personal Data to contractors without permission from the Finance Director. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

11 Sharing Personal Data within the School

11.1 This section applies when Personal Data is shared within the School.

11.2 Personal Data must only be shared within the School on a "need to know" basis.

11.3 Examples of sharing which are **likely** to comply with data protection legislation:

11.3.1 a teacher discussing a pupil's progress with other members of staff (for example, to ask for advice on how best to support the pupil);

11.3.2 informing an exam invigilator that a particular pupil suffers from panic attacks; and

11.3.3 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

11.4 Examples of sharing which are **unlikely** to comply with the Act:

11.4.1 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

11.4.2 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

11.5 You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the HR Manager as a matter of urgency.

12 Individuals' rights in their Personal Data

12.1 People have various rights in their information.

12.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Finance Director.

(a) Please let the Finance Director know if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information the School holds about them or their child;

(ii) asks to withdraw any consent that they have given to use their information or information about their child;

(iii) wants the School to delete any information;

(iv) asks the School to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for electronic information which they provided to the School to be transferred back to them or to another organisation;

(vi) wants the School to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the School newsletter or alumni events information; or

(vii) objects to how the School is using their information or wants the School to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

13 Requests for Personal Data (Subject Access Requests)

13.1 One of the most commonly exercised rights mentioned in section 12 above is the right to make a subject access request. Under this right people are entitled to request a copy of the

Personal Data which the School holds about them (or in some cases their child) and to certain supplemental information.

13.2 Subject access requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always immediately let the Finance Director know when you receive any such requests.

13.3 Receiving a subject access request is a serious matter for the School and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

13.4 When a subject access request is made, the School must disclose all of that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this should not deter staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues, pupils or students, in accordance with the School's other policies particularly in relation to safeguarding matters. Grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

14 Avoiding, mitigating and reporting data breaches

14.1 One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

14.2 In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, ArtsEd must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify the Finance Director. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

15 Breach of this policy

15.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

15.2 A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.