

|  |  |
| --- | --- |
| **Policy Title:** | Data Protection Policy |
| **Approved By:** | Colours Academy |
| **Author:** | Victoria Poole-Birrell |
| **Position:**  | Head of Centre |
| **Last Up-Dated**: | September 2019 |
| **Review Date:** | September 2020 |

1  INTRODUCTION  Colours Academy keeps information about staff, students and other parties to allow it to operate as a successful Further Education institution and meet its legal obligations. To comply with the Data Protection Act 1998 (“the Act), personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Academy must comply with the Data Protection Principles in the Act.

2  DATA PROTECTION PRICIPLES

In summary, the Head of Centre state that personal data shall:

1. Be processed fairly and lawfully.
2. Be obtained for specified and lawful purposes, and will not be processed in a manner incompatible with those purposes.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and up to date.
5. Not be kept for longer than is necessary.
6. Be processed in accordance with the rights of the person that the data is  about.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area, unless the country has equivalent protection for personal data.

3 PERSONAL DATA AND PROCESSING

Personal data is data relating to a living person who can be identified from that data whether stored electronically, in a paper-based filing system or in any other form or medium. Processing, for the purpose of the Act, is any operation on personal data including accessing, altering, adding to, using, disclosing, merging, deleting or destroying data.

4 DATA PROTECTION OFFICER

4.2  The designated Data Protection Officer is the individual or individuals appointed by the Academy to carry out the day to day duties. The Academy has one designated Data Protection Officers: the head of centre . They may be contacted at Colours Academy, c/o The Clay Factory, Redlake Industrial estate, Ivybridge, Devon, or by email (victoria@colours.academy).

 4.3  The Data Protection Officer will review the number and nature of requests for rights of access to data and queries raised in connection with this Policy annually and, in the light of this review, will propose any necessary changes to this Policy or related procedures.

5 REQUIREMENT TO COMPLY

5.1  Staff, students or other parties (e.g. contractors, consultants, partners) who process personal data collected in the name of the Academy must ensure that they follow the above Principles.

5.2  Compliance with the Act is the responsibility of all staff and students who access Academy systems. A breach of this Policy may lead to disciplinary action and/or access to Academy facilities being withdrawn, or criminal prosecution.

5.3  Questions about the interpretation or operation of this policy should be taken up with the Academy’s designated Data Protection Officer.

5.4  Staff, students or other parties who believe that the Policy has not been followed in respect of their own personal data should first raise the matter with the designated Data Protection Officer. If the matter is not resolved it may be raised as a formal complaint or grievance, in accordance with Academy procedures.

6 NOTIFICATION OF DATA HELD AND PROCESSED

6.1 Staff, students and other persons about whom the Academy holds data are entitled to:

Know what information the Academy holds and processes about them and why.

* Know how to gain access to it.
* Know how to update it.
* Know how the Academy complies with the Act.

6.2 The Academy will notify staff, students and other relevant parties of the nature of data that the Academy holds and processes about them, the reasons for which it is processed and how this can be changed.

7 RESPONSIBILITIES OF STAFF

7.1  Staff are responsible for:

Checking the information that they provide to the Academy in connection with their employment is accurate and up to date.

* + Informing the Academy of changes to information they have provided.

Checking information that the Academy sends to them, detailing data stored  and processed about them.

Informing the Academy of errors or changes in information stored. The  Academy cannot be responsible for un-notified errors.

* + Ensuring that personal data they hold about students is kept securely
	+ Inform the Data Protection Officer of any new uses of personal data
	+ Comply with the Academy’s IT Access, Usage and E-Safety Policy

Not disclosing any personal data, which they hold on students to an  unauthorised third party without consent

Destroying personal data in accordance with Academy Archive and Data  Retention Guidelines

7.2  If staff process information about other parties, they must comply with the guidelines for staff, detailed in Appendix 1.

7.3  Managers have a responsibility to ensure that their staff are aware of this policy receive appropriate training to enable them to comply with Data Protection Principles and adhere to retention periods to ensure that personal data is not kept for longer than is required.

8 RESPONSIBITIES OF STUDENTS

8.1  Students are responsible for:

Checking the information that they provide to the Academy in connection with their enrolment/studies is accurate and up to date

* + Informing the Academy of changes to information they have provided
	+ Complying with all academy policies regarding the use of IT.

8.2  Students may process personal data. If they do so they must notify their teacher or tutor, who must notify the designated Data Protection Officer. A learner, teacher or tutor who requires further clarification about this should contact the designated Data Protection Officer.

9 DATA SUBJECT CONSENT

9.1  In many cases, the Academy can only process personal data with the consent of the individual concerned. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Aacdemy processing specified classes of personal data is a condition of acceptance of a learner onto a course and a condition of employment for staff.

9.2  The Academy has a legal obligation to ensure that staff are suitable for the duties and responsibilities of their role, and students for the course offered. The Academy also has a duty of care to all staff and students and must therefore make sure that staff and those who use Academy facilities do not pose a threat or danger to themselves or others.

9.3  The Academy also asks for certain information about the health of staff and students, which it will only use in connection with the protection of the health and safety of the individual and others, but needs consent to process.

10 PROCESSING SENSITIVE INFORMATION

10.1  It is sometimes necessary for the Academy to process sensitive information, such as about a person’s health, criminal convictions or race. Sensitive personal data, as defined by the Act, includes information about:

* + racial or ethnic origins;
	+ political opinions;
	+ religious beliefs;

trade union membership (or non-membership);

* + physical or mental health or condition;
	+ sex life or sexual orientation;
	+ criminal (or alleged criminal) activities; or

criminal proceedings, criminal convictions (or any sentences imposed by the courts).

10.2  Sensitive personal data will be used only for the purpose it was collected such as managing the Academy’s equality and diversity policy and related statutory obligations, recruitment, ascertaining suitability and fitness for the job or course place, managing attendance and liaison with the Young People’s Learning Agency, the Skills Funding Agency or other regulatory authorities or funding providers. More information about this is available from the designated Data Protection Officer

10.3  If a person obtains a Gender Recognition Certificate while employed by or studying at the Academy, all records will be replaced with new details as soon as practicable. Regardless of the legal status of any individual, confidentiality regarding any previous gender identity will be maintained and any records that may be held by Academy, which could potentially reveal a change of status will be regarded as sensitive and access restricted.

11 DATA SECURITY

11.1  Staff are responsible for ensuring that personal data that they hold on behalf of the Academy is (a) secure, and (b) is not disclosed to an unauthorised third party. Any member of staff that processes personal data is a Data Processor under the Act.

11.2  Unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

11.3  Personal information should be physically secure and, if it is computerised, it should be coded, encrypted or password protected or kept only on a medium that is stored securely.

12 RIGHTS TO ACCESS INFORMATION

Staff, students and other parties have the right to access their personal data that is stored by the Academy.

13 EXAMINATION RESULTS

Students are entitled to information about their results for coursework and examinations. However, this may take longer than other information to provide if third parties such as examining bodies have to be contacted.

STAFF GUIDELINES FOR DATA PROTECTION

1  Most staff process data about students, e.g. when marking registers, or Academy work, writing reports or references, or as part of pastoral or academic supervisory roles. The Academy will ensure that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the Act. This information that staff deal with on a day-to-day basis will be “standard” and covers categories such as:

* + General personal details e.g. name and address.

Details about class attendance, course work marks, grades and associated comments.

Notes of personal supervision, including matters about behaviour and discipline.

2  Information about a student’s physical or mental health, gender identity, sexual orientation, political or religious views, trade union membership, criminal record, ethnicity or race is sensitive and can only be collected and processed with the student’s consent.

3  All staff have a duty to make sure they comply with the Data Protection Principles in the Data Protection Policy. In particular, staff must ensure that records are:

* + Accurate
	+ Up-to-date
	+ Fair
	+ Stored and disposed of securely, and in accordance with Academy
	+ Policy.

4  Staff must not disclose personal data to any student or third party, other than the person whom the data is about, unless for normal academic or pastoral purposes, in accordance with Academy policy, or as required by law.

5  In situations where third parties such as contractors, consultants or partners may have access to personal data that is the responsibility of the Academy then the member of staff who authorises access to this data should ensure that the third party is aware of the requirements of the Data Protection Policy.

6  Staff should not disclose personal data about other staff except in accordance with Academy policy or if the requesting employee needs the information to perform their duties. Only Academy Management can provide employment references to a prospective employer, a financial reference or similar. These will be co-ordinated and centrally recorded by the Personnel Section.

7  Personal data must not be given to someone you do not know unless you can confirm the identity the person requesting the information and satisfy yourself that you can legally comply with the request. Particular care should be taken with telephone requests and alleged relatives of students and staff. Sensitive personal data must not be disclosed without the express permission of the data subject. Refer all difficult situations to the designated Data Protection Officer.

8  Police or similar legal requests for disclosure of personal data should be referred to the designated Data Protection Officer. If the officer will not wait because the

matter is urgent, the officer must issue a DP1 form. This will detail the required information and must be signed by a Superintendent. You should make a note of the officer’s identification number, the information released and the date and time.

9  Personal data collected for a specified purpose should not be used for another purpose (e.g. unsolicited direct marketing).

10  Particular care should be taken with the use of E-mail or fax to transmit personal data. You will need to be certain that it has only been sent to the intended recipient. If you are the recipient, you will need to ensure that the data is retained for the appropriate length of time, remains accurate and can be retrieved when required.

11  Staff have screen-based access through the Academy IT facilities to a considerable amount of personal data that is held within the central information systems. Paper-based reports are also produced from these systems. Users should ensure that only authorised persons are able to see this information.

12  Before processing personal data, consider the following checklist:

Do you really need to record the information?

Is the information “standard” or “sensitive”?

* + If it is sensitive, has the data subject’s express permission been
	+ obtained?
	+ Does the data subject know why this data will be processed?
	+ Has the data subject confirmed that the data is accurate?
	+ Are you authorised to collect, store, process the data?

**13**  When you process data, simple security measures are:

File personal data away from sight of unauthorised persons.

* + Lock personal data away and/or lock the room if it is being left empty.

Do not leave personal data (paper based or on other media such as floppy disc, CD or pen drive) in bags or cases in situations where it may be mislaid, damaged or stolen. If possible, avoid taking such information off site.

Seal personal data transmitted by post (internal as well as external) in envelopes or packages.

Ensure your computer password is secure and not disclosed to anyone else.

* + Log out before you leave your computer unattended.
	+ Position computer screens away from unauthorised view.
	+ Set your computer screen saver to come on after a short interval.
	+ Have back-ups for personal data stored on computer.

Ensure that personal data being disposed of cannot fall into the wrong hands before it is finally destroyed. Shredding is more secure.

**14** Issues addressed to the designated Data Protection Officer. The most frequent issues are:

concerning compliance with the Data Protection Policy should be

(a)  periods for retention of records and

(b)  to notify the designated Data Protection Officer that personal data is being  collected, processed and stored.

**15** The designated Data Protection Officer is the Head of Centre. They may be contacted at the Colours Academy, c/o The Clay Factory or by e-mail.