Data Protection Policy

Reviewed by the Resources Committee, September 2023

• Introduces sanctions for breaches of the Regulation

2. The six principles of the Data Protection Act 2018

Principle 1: Personal data must be processed fairly and lawfully and in a transparent

manner.

Principle 2: Personal data must be processed for specific, explicit and legitimate purposes

that are compatible with the original purpose of obtaining it.

Principle 3: Data collected and stored must be adequate, relevant and limited to what is

necessary.

Principle 4: Data must be accurate and kept up-to-date.

Principle 5: Data must not be kept for longer than necessary.

Principle 6: Data must be processed in a manner which ensures appropriate security.

3. Summary

• Information Macook Septame ATMICHOS Deta Protection Policy is available from the Data

Requests for access to personal data should be referred to the Data Protection Officer who will deal with it promptly and within a maximum of 15 school days from receiving the request.

use of e-mail, internet, telephone or other data that the member of staff may be using inappropriately. If monitoring is used for training purposes the individual will be made aware of this at the time.

7. Enquiries

Data Protection Act (ICO), (www.ico.org.uk)

8. Fair obtaining and processing

fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues

for both staff and students, available on each school website.

"Data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"Parent" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

9. Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs either School of a change of circumstances their computer (SIMS) record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the

10. Data adequacy and relevance

requested, the date of entry in the log will be the date on which sufficient information has been provided.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Access to CCTV Images are also covered by the Right of Access under the Data Protection Act 2018. A separate form is available for such requests, which is available from the Data Protection Officer. These requests will be subject to the same recording and processing as detailed above.

On receipt of the completed form, and subject to satisfactory identity verification, all Access Requests will be processed and completed by the relevant establishment before disclosure to the requester.

14. Authorised disclosures

The Trust will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Trust's authorised officers may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system or by any other Personnel. In such circumstances the engineer would be required to sign a non-disclosure form. Personnel working on behalf of the Academy or LA are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else including anything that suggests that they are, or have been, either the subject of, or at risk of, child abuse.

• Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, left on desks at the end of the day.

Overall, the security policy for data is determined by each Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act 2018. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

16. Miscellaneous

CCTV within school will only be in public areas, will not intrude on used for security purposes. Notices will be placed in school to ensure that all visitors and staff are aware of this.

The Trust will also ensure that any service providers used that will handle personal data for example HR or Payroll comply with the Data Protection Act 2018.

Any member of staff found to mishandle data or share personal data with unauthorised

malicious or reckless breaking of the Data Protection Act 2018 will be counted as gross misconduct and could result in dismissal. Under this Act you can also be criminally liable if

17. Appendix 1

Personal Data Subject Access Request

(Data Protection Act 2018 Articles 15 to 22)

Under the Data Protection Act 2018, you have a right to access data relevant to you. If you wish to access data about someone else then you shall require their written consent, which you must make available to us. You may be committing an offence to seek data about other individuals without their consent.

18. Appendix 2

CCTV Data Subject Access Request

(Data Protection Act 2018 Articles 15 to 22)

Under the Data Protection Act 2018, you have a right to access data relevant to you. If you wish to access data

19. Appendix 3