Data Protection Policy

Data Protection Officer: **Waqas Riaz** OMG Education 85 Commercial Street, London, E1 6BG Email: dpo@omgeducation.co.uk Tel: 0208 159 3838

1. Introduction

1.1 OMG Education (OMG) is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 The Organisation may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the local authority, other schools and educational bodies, and potentially youth services.

1.3 This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Organisation complies with the following core principles of the GDPR.

1.4 Organisational methods for keeping data secure are imperative, and OMG believes that it is good practice to keep clear practical policies, backed up by written procedures.

1.5 This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Legal framework

2.1 This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations
- School Standards and Framework Act 1998

This policy links to and should be read in conjunction with the following policies:

- Information Security Policy
- CCTV Policy
- Complaints Policy
- Data Quality Policy
- E-Safety Policy
- Password Policy
- Subject Access Request Procedures

2.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. Applicable data

3.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1 In accordance with the requirements outlined in the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

g) The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

5.1 OMG will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. We will provide comprehensive, clear and transparent privacy policies. Internal records of processing activities will include the following:

a) Name and details of the organisation
b) Purpose(s) of the processing
c) Description of the categories of individuals and personal data
d) Retention schedules
e) Categories of recipients of personal data
f) Description of technical and organisational security measures
g) Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

5.2 The Organisation will implement measures that meet the principles of data protection by design and data protection by default, such as:

a) Data minimisation.
b) Pseudonymisation.
c) Transparency.
d) Allowing individuals to monitor processing.
e) Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

6.1 A DPO will be appointed in order to:

- Inform and advise the Organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Organisation's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

6.2 An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6.3 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to Organisations.

6.4 The DPO will report to the highest level of management at the Organisation, which is the OMG Governing Body.

6.5 The DPO will operate independently and will not be dismissed or penalised for performing their task.

6.6 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

7. Lawful processing

7.1 The legal basis for processing data will be identified and documented prior to data being processed.

7.2 Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - Compliance with a legal obligation.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.

- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the Organisation in the performance of its tasks.)

7.3 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8. Consent

8.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.3 Where consent is given, a record will be kept documenting how and when consent was given.

8.4 The Organisation ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

8.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

8.6 Consent can be withdrawn by the individual at any time.

8.7 Where a child is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

9.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9.2 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
    - The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

9.3 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

9.4 Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Organisation holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.5 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

9.6 In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access

10.1 Individuals have the right to obtain confirmation that their data is being processed.

10.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3 The Organisation will verify the identity of the person making the request before any information is supplied.

- A copy of the information will be supplied to the individual free of charge; however, the Organisation may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10 Where a request is manifestly unfounded or excessive, the Organisation holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.11 In the event that a large quantity of information is being processed about an individual, the Organisation will ask the individual to specify the information the request is in relation to.

11. The right to rectification

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2 Where the personal data in question has been disclosed to third parties, the Organisation will inform them of the rectification where possible.

11.3 Where appropriate, the Organisation will inform the individual about the third parties that the data has been disclosed to.

11.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.5 Where no action is being taken in response to a request for rectification, the Organisation will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2 Individuals have the right to erasure in the following circumstances:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

b) When the individual withdraws their consent

c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

d) The personal data was unlawfully processed

e) The personal data is required to be erased in order to comply with a legal obligation

f) The personal data is processed in relation to the offer of information society services to a child

12.3 The Organisation has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

a) To exercise the right of freedom of expression and information

b) To comply with a legal obligation for the performance of a public interest task or exercise of official authority

c) For public health purposes in the public interest

d) For archiving purposes in the public interest, scientific research, historical research or statistical purposes

e) The exercise or defence of legal claims

12.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6 Where personal data has been made public within an online environment, the Organisation will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1 Individuals have the right to block or suppress the Organisation's processing of personal data.

13.2 In the event that processing is restricted, the Organisation will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3 The Organisation will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Organisation has verified the accuracy of the data
- Where an individual has objected to the processing and the Organisation is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction
- Where the Organisation no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4 If the personal data in question has been disclosed to third parties, the Organisation will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.5 The Organisation will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14.4 Personal data will be provided in a structured, commonly used and machine-readable form.

14.5 The Organisation will provide the information free of charge.

14.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7 The Organisation is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8 In the event that the personal data concerns more than one individual, the Organisation will consider whether providing the information would prejudice the rights of any other individual.

14.9 The Organisation will respond to any requests for portability within one month.

14.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11 Where no action is being taken in response to a request, the Organisation will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1 The Organisation will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Organisation will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Organisation can

demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4 Where personal data is processed for direct marketing purposes:

- The Organisation will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Organisation cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Organisation is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the Organisation will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1 Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2 The Organisation will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3 When automatically processing personal data for profiling purposes, the Organisation will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Organisation has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

17.1 The Organisation will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Organisation has considered and integrated data protection into processing activities.

17.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Organisation's data protection obligations and meeting individuals' expectations of privacy.

17.3 DPIAs will allow the Organisation to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Organisation's reputation which might otherwise occur.

17.4 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5 A DPIA will be used for more than one project, where necessary.

17.6 High risk processing includes, but is not limited to, the following:

a) Systematic and extensive processing activities, such as profiling
b) Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
c) The use of CCTV.

17.7 The Organisation will ensure that all DPIAs include the following information:

a) A description of the processing operations and the purposes
b) An assessment of the necessity and proportionality of the processing in relation to the purpose
c) An outline of the risks to individuals
d) The measures implemented in order to address risk

17.8 Where a DPIA indicates high risk data processing, the Organisation will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches

18.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2 The Governing Body and Principal will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed (see Appendix A).

18.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Organisation becoming aware of it.

18.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

18.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Organisation will notify those concerned directly.

18.7 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.9 Effective and robust breach detection, investigation and internal reporting procedures are in place at the Organisation, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.10 Within a breach notification, the following information will be outlined:

a) The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
b) The name and contact details of the DPO
c) An explanation of the likely consequences of the personal data breach
d) A description of the proposed measures to be taken to deal with the personal data breach
e) Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.11 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security (see also Information Security Policy)

19.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

19.4 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

19.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

19.6 All electronic devices are password-protected to protect the information on the device in case of theft.

19.7 Where possible, the Organisation enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.8 Staff and governors will not use their personal laptops or computers for Organisation purposes.

19.9 All necessary members of staff are provided with their own secure login and password.

19.10 Emails containing personal or sensitive information will be sent securely using the Secure Email Service.

19.11 Senders of any controlled/restricted email must be extremely vigilant about the recipients email address, so as to not send any sensitive data to the wrong individual/s. Senders of controlled/restricted emails, via any of these methods, must ensure they have and use the correct recipient email address

19.12 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.13 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Organisation premises accepts full responsibility for the security of the data.

19.14 Before sharing data (see Appendix B for procedure), all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

19.15 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Organisation containing sensitive information are supervised at all times.

19.16 The physical security of the Organisation's buildings and storage systems, and access to them, is reviewed on a termly basis as per the Organisation's Information Security Policy. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.17 OMG takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.18 The IT Manager is responsible for having continuity and recovery measures in place to ensure the security of protected data.

20. Publication of information

20.1 OMG publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information
- Governance information

20.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

20.3 OMG will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.4 When uploading information to the Organisation website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1 OMG understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2 OMG notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

21.3 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4 All CCTV footage will be kept for one month for security purposes; the IT Manager is responsible for keeping records and the Data Protection Officer is responsible for allowing access. Details are set out in the Organisation's CCTV Policy.

21.5 OMG will always indicate its intentions for taking photographs of learners and will retrieve permission before publishing them.

21.6 If OMG wishes to use images/video footage of learners in a publication, such as the Organisation website, prospectus, or showcases, written permission will be sought for the particular usage from the learner (or parent/guardian if under 18).

21.7 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Data retention

22.1 Data will not be kept for longer than is necessary.

22.2 Unrequired data will be deleted as soon as practicable.

22.3 Some educational records relating to former students or employees of the Organisation may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

23.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2 Data provided by the DBS will never be duplicated.

23. 3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Policy review

24.1 This policy is reviewed every two years by the Organisation's Governing Body.

APPENDIX A: Data Breach Procedure

A1. OMG holds personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by OMG and all Organisation staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

A2. This breach procedure sets out the course of action to be followed by all staff at OMG if a data protection breach takes place.

A3. Legal Context

Article 33 of the General Data Protection Regulations Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:

    (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

    (c) describe the likely consequences of the personal data breach;

    (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

A4. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of student, staff or governing body data and/ or equipment on which data is stored;

- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

A5. In the event that the Organisation identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Data Protection Officer, or, in their absence, the Principal. If the breach occurs or discovered outside normal working hours, this should begin as soon as is practicable.
2. The Data Protection Officer must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT manager.
3. The Data Protection Officer must inform the Principal and Chair of Governors as soon as possible. As a registered Data Controller, it is the Organisation's responsibility to take the appropriate action and conduct any investigation.
4. The Data Protection Officer must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the Organisation's legal support should be obtained.
5. The Data Protection Officer must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    - Attempting to recover lost equipment.
    - Contacting the relevant members of staff so that they are prepared for any potential
        - enquiries from parents, students or the press.
    - The use of back-ups to restore lost/damaged/stolen data.
    - If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

A6. In most cases, the next stage would be for the Data Protection Officer to fully investigate the breach. The Data Protection Officer should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data
- Its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (learners, staff members, suppliers etc.) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

A7. Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Data Protection Officer should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the centre is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Organisation's Complaints, Compliments and Concerns Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

A8. Once the initial aftermath of the breach is over, the Data Protection Officer should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

A9. The Data Protection Officer should ensure that staff are aware of the Organisation's Data Protection Policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Organisation's Data Protection Policy and associated procedures, they should discuss this with the Data Protection Officer.

For further information, see:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal- data-breaches/

APPENDIX B: Procedure for Sharing Information

B1. This procedure has been developed in accordance with the ICO's Data Sharing Code of Practice (2011) https://ico.org.uk/media/for- organisations/documents/1068/data_sharing_code_of_practice.pdf

B2. In order to share any personal data with third parties, authorisation must be gained from the Data Protection Officer by completing the form below.

B3. In an emergency situation where a person's vital interests are compromised the Academy reserves the right to share information with the relevant authorities.

Name	
Date	
Third Party Requesting Data	
Nature of Request	

Please outline the specific data to be shared

What is the objective in sharing the data?

Is there a legal basis for sharing the data?

Could the objective be achieved without sharing the data or anonymising it?

Are there specific arrangements for the retention period/deletion of data?

What risk does the data sharing pose?

Is the third party GDPR compliant?

DATA PROTECTION OFFICER TO COMPLETE

Can the data be shared?
Yes/No What is the justification:

Sharing log completed?

Should the person involved be informed, i.e. not covered by a prior privacy notice?

DPO Signature:	
Date:	