Data Protection Policy

Including:

Data Subject Access Request Policy

Data Incident Management Policy

Agreed by SLT: July 2023
Review: July 2024
Signed by:

Contents

1.0 Core Values and how they link with this policy 4
2.0 Introduction 5
3.0 Purpose 5
4.0 Scope of policy 5
5.0 Glossary 6
6.0 Responsibilities 7
6.1 Data Controller 7
6.2 Governing Board 7
6.3 Data Protection Officer (DPO) 7
6.4 Principal 7
6.5 Data Champions 7
6.6 All Staff 7
7.0 Links to other policies 8
8.0 Collecting personal data 8
8.1 Lawfulness, fairness and transparency 8
8.2 Limitation, minimisation and accuracy 8
9. Sharing and disclosing personal data 9
10. Data subject access requests and other rights of individuals 9
10.1 Data subject access requests 9
11. Parental requests to see the educational record 11
12. CCTV 11
13. Photographs and videos 11
14. Sharing information via email 11
15. Use of WhatsApp 12
16. Data protection by design and default 12
17. Data security and storage of records 13
18. Working off-premises 13
19. Disposal of records 13
20. Personal data breaches 14
21. Training 14

22. Monitoring and Review 14
Appendix 1: Data Subject Access Request (DSAR) Policy.....15
Appendix 2: Data Security Incident Management Policy 19

1.0 Core Values and how they link with this policy

think differently

The Data Protection Policy has been written to help foster an environment that embraces and celebrates difference and ensures that all pupils and staff are safe and embody practice that supports our Vision, Mission and Core Values. Staff at James Brindley Academy are expected to **THINK DIFFERENTLY** to inspire young people to overcome all barriers and achieve their dreams.

James Brindley Academy is committed to the principles of **ethical leadership** in implementing this policy, and this includes all employees respecting the rights of our young people as set out in the **UNICEF Charter.**

JBA Core Values	How this policy addresses these values
THRIVE – We create a positive environment where we thrive and succeed	The Data Protection Policy provides a clear framework for a safe working environment where individuals' data is secure and allows them to be free to progress and flourish.
HIGH ASPIRATIONS – We have high aspirations for ourselves and others	The Data Protection Policy sets the highest standards for individuals within the academy and has the approach of continual improvement.
INCLUSION – We are inclusive in all we do and celebrate our differences	The Data Protection Policy ensures all group and individual data is protected.
NURTURE – We educate our young people and staff to nurture their emotional health and wellbeing	The Data Protection Policy is designed to support individuals in understanding their role in data protection. This ensures our personal and corporate information is safe, so our mental health and wellbeing is not adversely affected.
KEEP SAFE – We ensure that keeping safe and the safety of others is paramount	The Data Protection Policy has safety at its core! Ensuring our data is safe through educating people within our Academy of our protocols and best practice.

2.0 Introduction

The Data Protection Policy is a statutory policy.

3.0 Purpose

James Brindley Academy aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018 https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/

This policy applies to all personal data, regardless of whether it is in paper, or electronic or any other format.

4.0 Scope of policy

This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. It also meets the requirements set out in the academy's funding agreement and articles of association.

This policy applies to all staff employed by the academy and to external organisations or individuals working on the academy's behalf. Staff who do not comply with this policy may face disciplinary action.

The UK GDPR is based on data protection principles that the academy must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the academy aims to comply with these principles.

5.0 Glossary

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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 • Sex life or 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. The identified or identifiable individual.
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.

6.0 Responsibilities

6.1 Data Controller

The academy processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.
The academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6.2 Governing Board

The governing board has overall responsibility for ensuring that the academy complies with all relevant data protection obligations.

6.3 Data Protection Officer (DPO)

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report their advice and recommendations on academy data protection issues to the governing board.

The DPO is also the first point of contact for individuals whose data the academy processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

The DPO is Kevin Biggs and is contactable via dpo@jamesbrindley.org.uk

6.4 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

6.5 Data Champions

Each centre has a data champion to promote increased awareness and knowledge of data protection requirements within the centre.

6.6 All Staff

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy of any changes to their personal data, such as a change of address
- Contacting their data champion in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- Contacting the DPO in the following circumstances:
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual (subject access requests), or transfer personal data outside the European Economic Area
    - If there has been a data breach or near miss and to report the incident via email to the DPO

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals or requires a 3rd party to process personal data
- If they need help with any contracts or sharing personal data with 3rd parties

7.0 Links to other policies

Bring Your Own Device Policy

8.0 Collecting personal data

8.1 Lawfulness, fairness and transparency

The academy will only process personal data where there is one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy 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 academy, 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 academy 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 pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with a privacy notice and any other relevant information required by data protection law.

8.2 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.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the IRMS Academies Toolkit.

9. Sharing and disclosing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil 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 pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so and in situations where we feel it is in the public interest to disclose certain information to the police including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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 pupils or staff. All 3rd party requests must be authorised by the DPO (unless in an emergency situation).

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. Data subject access requests and other rights of individuals

10.1 Data subject access requests

Individuals have a right to make a 'data subject access request' to gain access to personal information that the academy 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 isn't possible, the criteria used to determine this period
- 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
-

Data subject access requests must be submitted to the DPO. Any member of staff receiving a data subject access request must immediately forward it to the DPO.

10.2 Children and data 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 data 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 below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a data subject access request. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Data Subject Access Request Policy

The full policy can be found in Appendix 1 of this policy.

10.4 Other data protection rights of the individual

In addition to the right to make a data subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 DPO.

11. 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 pupil) within 15 school days of receipt of a written request.

12. 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 Facilities Manager.

13. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Sharing information via email

All emails which contain personal identifiable information (PII) should be constructed to ensure that PII is minimised.

Internal emails (name@jamesbrindley.org.uk to name@jamesbrindley.org.uk)

Where information is to be attached to an email sent using James Brindley email addresses, staff should ensure that a hyperlink to the document is used rather than a direct attachment. If the email

is sent incorrectly to an individual outside of the academy, they will be unable to access the information, reducing the risk of a data breach.

Remember that academy email accounts are included within Subject Access Requests and are monitored by the academy.

External emails (name@jamesbrindley.org.uk to non-James Brindley email)

Where PII is required to be emailed to a non-James Brindley email recipient, it must be sent using a secure mechanism. There are a number of ways this can be achieved

1. Using **JBSec** in the email subject line – this will encrypt and secure the email and any attachments. Recipients will be required to log in to access the email.

2. Egress – this is a secure system of transfer that can be used when communicating PII.

3. Encryption and password protection of an attachment – you can individually encrypt and password protect files prior to attachment. If you are sending information in this way, please remember not to include personal information in the email itself, as this will not be secure. The password should be sent using another method of communication, such as text.

15. Use of WhatsApp

WhatsApp is used as a form of communication at JBA. Any WhatsApp contacts between JBA staff must have the option for "disappearing messages every 7 days" enabled.

16. Data protection by design and default

The academy 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 (see section 6)
- 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
- 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, how and why we are storing the data, retention periods and how we are keeping the data secure

17. Data security and storage of records

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 personal data must not be left on office and classroom desks, on staffroom tables or pinned to notice/display boards
- Where paper-based personal information needs to be taken off site, the minimum of information is to be taken and the rationale for it noted along with details of what is being taken and the risks associated with losing it. A lockable bag must be used and kept by the member of staff, not left in a car. The information must be returned to the centre and re-filed as quickly as possible. In the event the data is lost every effort must be made to find it by re-tracing the member of staff's movements.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment and to implement the Bring Your Own Device Policy.
- 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 (see section 8)

18. Working off-premises

Staff who are required to work off James Brindley premises need to adhere to normal data security practices. Additionally, staff need to be mindful of:

- Ensuring that papers, screens and conversations are kept private
- Only using authorised devices with up-to-date software
- Keeping personal data separate from academy data
- Keeping academy equipment as secure as possible within the environment
- Not using public wi-fi

19. 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.

20. Personal data breaches

The academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the policy set out in appendix 2.

When appropriate, the data breach will be reported to the ICO within 72 hours.

21. Training

All staff and trustees are provided with data protection training as part of their induction process. As a minimum, staff will receive annual update training and are required to read this policy on an annual basis.

22. Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy in line with legislative changes and best practice. All staff are encouraged to suggest improvements to data protection working practices to the DPO.

Appendix 1: Data Subject Access Request (DSAR) Policy

CONTENTS

1. Context
2. Purpose
3. Data subject's rights
4. Recognising a data subject access request (DSAR)
5. Business as usual requests
6. Receiving a DSAR
7. Validating a DSAR
8. Fees & charging
9. Logging & acknowledging a DSAR
10. Requests for CCTV images/footage
11. Reviews
12. Staff training

1. Context

This policy applies to all James Brindley Academy staff who either have access to personal data or who may come into contact with our partners or contractors.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) provide data subjects with a variety of rights in relation to the personal data held about them by James Brindley Academy. One of these rights allows access to their personal data processed (held) by the Academy.

Data subjects have the right to appeal to the Information Commissioner's Office (ICO) about any decision made by James Brindley Academy in response to any data subject request. In the event the ICO finds that an organisation has infringed rights of a data subject, the Academy could be exposed to ICO action including a monetary penalty of the higher of 4% of its annual global turnover or €20M. Therefore, it is important that we treat all individuals fairly and each data subject request is handled in accordance with this policy.

Members of staff should immediately contact the Data Protection Officer (DPO) if they receive a data subject access request.

2. Purpose of this policy

2.1 To ensure that the Academy complies with its obligations under the General Data Protection Regulation 'Right of Access'.

2.2 To ensure that all staff are aware of their responsibilities in relation to data subjects exercising the right of access.

2.3 To establish consistency in the handling of DSARs across the Academy.

3. Data subjects rights

The purpose of a data subject access request is to allow individuals to confirm the accuracy of personal data and check the legality of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any personal data that the Academy holds about them which includes copies of email correspondence and database entries referring to them or opinions expressed about them.

4. Recognising a data subject access request (DSAR)

Any written or verbal request for a copy of the data subject's own personal data should be treated as a potential data subject access request (DSAR), irrespective of who in the Academy has received it. The nature of the request will dictate whether it is best dealt with as a formal data subject access request, or responded to as 'business as usual'.

5. Business as usual requests

Whilst the data subject access rights technically apply once a valid request has been received, a pragmatic approach should be taken to dealing with individuals who request information in writing; for example, an email asking for confirmation of their contracted terms and conditions may constitute

a DSAR, but would be best dealt with as a business-as-usual enquiry and responded to quickly, in accordance with relevant organisational processes.

6. Receiving a DSAR

When a DSAR is received the request must be forwarded immediately to the Data Protection Officer dpo@jamesbrindley.org.uk All DSARs received by James Brindley Academy will be managed by the Data Protection Officer (DPO) who will work with appointed staff to complete the request within the statutory deadline of one calendar month.

7. Validating a DSAR

Upon receipt of a DSAR, the DPO will work with the team responsible for processing the request to check that the request is valid. For a DSAR to be valid, the requester must:

1. Put their request in writing (reasonable adjustments must be made to take account of any disabilities and health issues)
2. Provide sufficient clarity in their request to enable us to determine whether we are processing the requested data, and to locate it
3. Satisfy us of their identity

8. Fees & charging

8.1 Under the UK GDPR, the Academy must provide a copy of the information free of charge.

8.2 A 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. The ICO have provided no guidance on what they consider to be excessive.

8.3 A fee may also be charged for requests for further copies of the same information, but a charge should not ordinarily be levied for all subsequent access requests.

8.4 The fee must be based on the administrative cost of providing the information.

9. Logging and acknowledging a DSAR

9.1 DSARs must be assigned a unique reference number and recorded on a log.

9.2 If any validation checks are outstanding (e.g. the requester has not provided proof of ID) then this should be requested after the request has been logged. The 1 calendar month response timeframe does not begin until the request has been validated.

9.3 Once the request has been validated, an acknowledgement should be sent to the requester confirming receipt of the request and providing the requester with the reference number and deadline for the response.

10. Requests for CCTV images/footage

10.1 Requests for copies of CCTV footage, where the requester is present in the footage, must be dealt with as a formal data subject access request by the DPO. The DPO must be satisfied that the request is from the individual in the footage, and seek adequate proof of this.

10.2 Requests for CCTV images showing property damage or a suspected criminal offence, where the requester was not present at the time of the incident, should not be dealt with as a subject access request. Such data may only be released to the police, or to the requester's insurance company.

10.3 CCTV footage is ordinarily only kept for 30 days, therefore any request for CCTV footage must be immediately notified to the Facilities Manager to ensure that the requested footage is not destroyed.

11. Reviews

11.1 Where a requester expresses dissatisfaction with the handling of their request, then a review must be conducted by a suitably experienced individual. Where the request was processed by an individual other than the DPO, the reviewing individual should contact the DPO for advice.

11.2 The review must seek to determine whether the requester's right of access has been upheld.

Examples of reasons for seeking a review include, but are not limited to:

- that the response was not issued within the statutory timeframe
- that all the requested information was not supplied
- that the application of an exemption could not be justified
-

11.3 Reviews must be concluded, and a response provided to the requester within 21 working days.

12. Staff training

12.1 All staff will complete mandatory Data Protection Training on an annual basis. This training will explain what a DSAR is, how to recognise one and what to do if you receive one.

12.2 The DPO may provide additional face-to-face training to those staff responsible for any part of the DSAR handling procedure, from logging/acknowledging a DSAR, through to making a disclosure or conducting a review if it is required.

Appendix 2: Data Security Incident Management Policy

Contents

1. What is covered
2. What you must do
3. Failure to notify
4. Why you must notify
5. What happens once you have reported the breach

1. What Is Covered

1.1 This policy covers what are commonly referred to as data breaches and near misses. This includes any loss of data where we are the data controller (data owner) or an incident occurs which could have resulted in the loss of data (a near miss). Examples include:

- Loss of a computer, laptop, mobile telephone or removable storage media
- Loss of our data stored on a computer or server due to corruption of the hard drive
- Loss of physical papers or files containing our data
- Hacking of our computer network and systems or a computer network and system that processes data for us
- A ransomware, malware, virus or other malicious code attack made to our computer network and systems
- Non secure destruction of our data (putting confidential paper waste in the recycling)
- Sending an email or post to the wrong person which contains our data
- Sending an email to a group of recipients using the "to" field when their email addresses should not have been disclosed to the other recipients
- Allowing someone to overhear a telephone conversation when identifying details are disclosed
- Data being disclosed or revealed to someone else in the organisation (or another organisation) who is not entitled to see or know that data
- Entering incorrect data against a record, for example making an entry on the wrong customer record
- Mis-addressing a letter which contains the data of a third party

1.2 The above is not an exhaustive list, and data breaches can take many forms. If anything involves loss of our data or unauthorised access to our data and that data relates to an individual in any way, then it will be classified as a data breach under data protection laws. The academy requires the reporting of all data breaches, whether the data relates to an individual or is corporate data.

1.3 Compliance with policies and operational procedures in respect of data handling and security are critical.

2. What You Must Do

2.1 All data breaches and near misses must be reported within 2 hours of the incident being identified. You must email biggsk@jamesbrindley.org.uk, murgatroydj@jamesbrindley.org.uk and dpo@jamesbrindley.org.uk

2.2 If the incident is considered serious (high risk) then the Data Protection Officer must also be verbally contacted.

2.3 Inform your line manager.

2.4 The operation procedure “Data Security Incident Management Procedure” must be followed when reporting and managing any such incident.

3. **Failure to Notify**

3.1 If you notify a data breach in accordance with this policy, then even if you are at fault in causing or contributing to the data breach, for example due to human error, then we would prefer to know about the data breach. The fact that you have reported it will work in your favour, and it is a fact of life that data losses sometimes occur, often due to human error or the need to improve our systems and procedures.

3.2 However if you are aware of a data breach and you fail to follow procedures in accordance with this policy, then we will regard it as serious misconduct and we may use the Disciplinary Policy.

3.3 If you are a third-party supplier to us, and you are aware of a data loss in relation to our data or data we process on behalf of a third party and you fail to notify us of the data loss in accordance with this policy, then we will regard that as a material and serious breach of contract.

3.4 This applies whether the data loss was caused or contributed to by you or if you are just aware of a data loss caused or contributed to by a colleague or third party or even just aware of a data loss where no-one was at fault.

4. **Why You Must Notify**

4.1 Under Data Protection laws we are under a duty to inform the regulator (the Information Commissioner’s Office; ICO) of data breaches involving personal data of which we are the data controller within 72 hours in cases where the data loss may result in harm to individuals.

4.2 Your notification of a data breach will allow us to assess whether we need to inform the ICO regarding the data breach. It is the responsibility of the Principal with the support of the Data Protection Officer to decide if a breach should be reported to the ICO. You must never report a breach to the ICO.

4.3 If we fail to notify the ICO when we should then we can be subject to fines of up to 2% of group worldwide turnover or 20 million euros, whichever is the higher. These are very substantial risks and for this reason the failure to notify us of any data loss which you are aware of is treated as serious misconduct, and could result in dismissal or termination of a contract.

4.4 Also if we are processing data on behalf of a third party, then that third party will require us to inform them of the data loss involving their data as soon as possible as they will be subject to the same risks. It is also a legal requirement under Data Protection laws that we do this as soon as possible. If we do not, then as well as breaching the contract with the third party, we can also be liable for the same level of fines as if it were our data.

5. **What Happens Once You Have Reported the Breach**

5.1 Once you have reported a data breach, the Data Protection Officer, and if necessary your line manager, will assess what needs to happen next. This may be that we have to undertake a more

detailed investigation, in which case we may need you to provide further detailed information regarding the incident.

5.2 We may also need to report the data loss to the individuals whose data is affected by the data breach. The decision to do this will be made by the Data Protection Officer.

5.3 We may also need to take steps to try to mitigate the impact of the data breach, contain the data breach or reverse the data breach. These steps are easier to take if we know about the data breach as soon as possible and without any delays.

5.4 We may also need to change our systems, procedures and security to prevent or reduce the risk of such a data loss occurring in the future. There is always something to be learnt from a data breach.

5.5 Irrespective of the seriousness of the data breach or near miss we will record the incident on our data breach register, which may help us to spot patterns or areas of particular risk over time so that we can take steps to prevent or reduce the risk of repeat data losses.