The Romero Catholic Academy
Nurturing the Talent of Tomorrow

Data Protection Policy

Responsible for policy:	**CC2**
Date of policy:	**September 2019**
Date approved by CC2:	**September 2019**
Date of review:	**September 2022**
Policy Status:	**Statutory**
Chair of Directors	

The Romero Catholic Academy
Nurturing the Talent of Tomorrow

Contents

Definitions 3

1. Aims 4
2. Legislation and guidance 4
3. Definitions 4
4. The data controller 5
5. Roles and responsibilities 5
6. Data Protection Principles 6
7. Collecting personal data 7
8. Sharing personal data 7
9. Subject access requests and other rights of individuals 8
10. Biometric recognition systems 10
11. CCTV 11
12. Inventry Ltd 11
13. Photographs and videos 11
14. Data protection by design and default 12
15. Data security and storage of records 12
16. Disposal of records 13
17. Personal data breaches 13
18. Training 13
19. Links with other policies 13
20. Monitoring and Review 13

Appendix 1: Personal Data Breach Procedures 14

Definitions

In this **Data Protection Policy**, unless the context otherwise requires, the following expressions shall have the following meanings:

i '**The Romero Catholic Academy**' means the Company named at the beginning of this **Data Protection Policy** and includes all sites upon which the Company is undertaking, from time to time, being carried out. The Romero Catholic Academy includes; **Corpus Christi**, **Good Shepherd**, **Sacred Heart**, **Blue Sky**, **SS Peter and Paul**, **St Gregory**, **St John Fisher**, **St Patrick**, **Cardinal Wiseman**, **Shared Services Term**.

ii '**Romero Catholic Academy'** means the Company responsible for the management of the Academy and, for all purposes, means the employer of staff at the Company.

iii '**Board'** means the board of Directors of the Romero Catholic Academy.

iv '**Chair'** means the Chair of the Board or the Chair of the Local Academy Committee of the Academy appointed from time to time, as appropriate.

v '**Clerk'** means the Clerk to the Board or the Clerk to the Local Academy Committee of the Academy appointed from time to time, as appropriate.

vi '**Catholic Senior Executive Leader**' means the person responsible for performance of all Academies and Staff within the Multi Academy Company and is accountable to the Board of Directors.

vii '**Diocesan Schools Commission**' means the education service provided by the diocese, which may also be known, or referred to, as the Birmingham Diocesan Education Service.

viii '**Local Academy Committee**' means the Academy Committee of the School.

ix '**Academy Committee Representatives'** means the governors appointed and elected to the Local Academy Committee of the School, from time to time.

x '**Principal'** means the substantive Principal, who is the person with overall responsibility for the day to day management of the school.

xi '**School'** means the school or college within The Romero Catholic Academy and includes all sites upon which the school undertaking is, from time to time, being carried out.

xii '**Shared Services Team'** means the staff who work in the central team across the Company (e.g. HR/ Finance)

xiii '**Vice-Chair'** means the Vice-Chair of the Academy Committee elected from time to time.

xiv **'School DPO'** means the Data Protection Officer responsible for all schools within The Romero Catholic Academy (Warwickshire Legal Services)

1. Aims

The Romero Catholic Academy aims to ensure that all personal data collected about staff, pupils, parents, directors, local academy committee members, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

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.

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.

4. The data controller

The Romero Catholic Academy processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

The Romero Catholic Academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by The Romero Catholic Academy and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Academy Board of Directors

The Academy Board of Directors has overall responsibility for ensuring that The Romero Catholic Academy complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for providing advice and guidance to The Romero Catholic Academy in order to assist The Romero Catholic Academy to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of The Romero Catholic Academy data processing activities and report to the Academy Board of Directors their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is the School DPO Service provided by Warwickshire Education Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

5.3 Principal

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

5.4 The Academy Business Director, Academy Data Protection Champion and School Data Protection Officers

The Romero Catholic Academy has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer;

- Laura Morgan Academy Data Protection Champion who is contactable via l.morgan@romeromac.com or 02476 451888
- Patrick Taggart Academy Business Director who is contactable via p.taggart@romeromac.com or 02476 451888

5.5 All staff

All members of staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the designated Principal, School Data Protection Champion, Academy Business Director, or the Academy Data Protection Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - 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, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that our Academy must comply with.

The Romero Catholic Academy has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
2) used for specified, explicit and legitimate purposes ('purpose limitation');
3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');
5) kept no longer than is necessary ('storage limitation');
6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how The Romero Catholic Academy aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Romero Catholic Academy shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to The Romero Catholic Academy to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school 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 school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- 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 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 the relevant information required by data protection law.

7.2 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 guidance set out in the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else except as set out in The Romero Catholic Academy's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared 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, 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.

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.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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

Subject access requests may be submitting in writing or verbally and can be sent either to the Data Protection Officer, a member of staff or a Governor / Trustee. To enable the request to be accurately responded to, the applicant should be encouraged to make the request in writing and to set out:

- Name of individual
- Name of School
- Correspondence address
- Contact number and email address
- Details of the information requested

The School DPO will send the subject access request to the Academy Data Protection Champion. If staff receive a subject access request they must immediately forward it to the school Data Protection Champion (School Business Manager/Office Manager/Operations Manager). The school will then forward to Laura Morgan at The Romero Catholic Academy C/O Cardinal Wiseman Catholic School, Potters Green Road Coventry CV2 2AJ or l.morgan@romeromac.com who will ensure that the School DPO Service is informed.

Information to be released will be collated by the School and then sent to the School DPO Service for checking and sending out to the applicant.

9.2 Children and 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 subject access request with respect to their child, the person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at our school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see 9.3), 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, where processing is based on the consent of the pupil or parent
- 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 Data Protection Champion who will send it to the DPO for information purposes.

10. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Romero Catholic Academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use The Romero Catholic Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners via Parentmail at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We also use video and audio data for training and professional development purposes. 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 Laura Morgan, Academy Data Protection Champion.

Please refer to our CCTV policy on www.romeromac.com for further details

12. Inventry Ltd

As part of our security and safeguarding procedures the schools are installed with visitor management software called Inventry Ltd. It is a fully equipped integrated solution which allows the schools to accurately monitor who is in school at any one time. Inventry speeds up the sign in process, identity information is kept secure and it keeps our pupils and staff safe.

All visitors are asked to sign in using Inventry and this will ask for a full name and take a photograph of the visitor. The visitor will wear the badge for the duration of the time spent in the school to ensure visitors are visible to all pupils and members of staff.

The system will also take a photograph of persons signing pupils in or out of the school, outside of standardised hours. A prominent sign in each school main reception explains this is in place for safeguarding purposes.

Please refer to Inventry GDPR policies and FAQ's for further information https://inventry.co.uk/gdpr-policies/

13. Photographs and videos

As part of our school activities, The Romero Catholic Academy may take photographs and record images of individuals within the School.

The Romero Catholic Academy 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 The Romero Catholic Academy need parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where The Romero Catholic Academy don't need parental consent, it shall clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, local radio, campaigns
- Online on our school 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.

See our school application packs for more information on our use of photographs and videos.

14. Data protection by design and default

The Romero Catholic Academy shall put measures in place to show that it has integrated data protection into all of its 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
- 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

15. Data security and storage of records

The Romero Catholic Academy 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 confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the Information Security 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)

16. 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, The Romero Catholic Academy 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.

17. Personal data breaches

The Romero Catholic Academy shall take all reasonable steps to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, The Romero Catholic Academy shall report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- HR – Disciplinary Policy
- Freedom of Information Policy
- CCTV Policy
- Romero Privacy Notices
- Any other individual school policies linked to information security and E-Safety

20. Monitoring and Review

The Board of Directors delegate the implementation of this policy to the Academy Committee.
This policy will be reviewed by CC2 Strategy, People and Organisational Development.

Appendix 1: Personal Data Breach Procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, The Romero Catholic Academy will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.
2. Examples of how a breach may occur include:
    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.
3. If any member of staff of The Romero Catholic Academy, or Director or Local Academy Committee Representative discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to inform The Romero Catholic Academy's;
    - Laura Morgan Data Protection Champion l.morgan@romeromac.com or 02476 451888
    - Patrick Taggart Academy Business Director p.taggart@romeromac.com or 02476 451888.
4. Upon being notified, The Romero Catholic Academy's Data Protection Officer will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of The Romero Catholic Academy, then the Academy's Data Protection Officer will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.
5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All Academy staff and Directors / Local Academy Committee Representatives are expected to work in partnership with the Data Protection Officer in relation to the following matters

Notification of Breaches

Any member of staff or Director / Local Academy Committee Representative who becomes aware of a personal information breach should provide full details to the Data Protection Officer for the Academy within 24 hours of being made aware of the breach. The Data Protection Officer will then complete the Data Breach Record Form and Incident Log. When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Officer should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data have been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the Academy?

All staff and Directors and Local Academy Committee Representatives should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.