Subject:	**Confidentiality and Data Protection**	Number:	**POL00108**
		Type:	**Policy**
Approved by:		Issued:	**October 2021**
		Revision:	**2.1**
	Managing Director	Effective:	**October 2023**

1. Objectives

The Robert Holme Academy recognises its responsibilities in managing data and records for staff, pupils, parents and all stake-holders to prevent loss, damage or unauthorised disclosure. We act proactively and at all times to ensure personal data is collected and stored for legitimate purposes only and is processed lawfully, fairly and in a transparent manner. Personal data is only collected, stored and retained for as long as is necessary to fulfil any contractual and legal obligations.

Obsolete records and data, including paper and electronic records are destroyed in a securely to prevent reuse and unauthorised disclosure. Obsolete paper records are shredded and computer media containing personal data (including faulty devices) is physically destroyed to prevent unauthorised access.

Wherever possible personal data and records are only held in local files and on encrypted local devices in secure areas within the premises, except for backup purposes. Documents and media (including backup devices) are stored securely in locked facilities.

Personal data is not released to unauthorised third parties and is only shared on an exceptional basis, such as to support a criminal investigation or to support a safeguarding concern.

Our policy is reviewed not less than every year or in the light of legislative or substantial organisational change and continual improvement.

2. Scope and Applicability

This policy is applicable to all members of staff and mandates the practices necessary to ensure personal data is managed effectively and securely to minimise loss, damage or unauthorised disclosure.

The policy and procedures identified within this document apply to all possible sources data and personal records including paper and/or electronic information relating to staff, pupils, parents and all other stake-holders.

Where personal includes, but is not limited to:

- name;
- address;
- contact details (telephone numbers, email etc.);
- usernames, IDs and biometric information;
- ethnic and racial background;
- trade union, political affiliations and religious beliefs;
- employment details - including salary information, disciplinary records, etc.;
- health records;
- performance records;
- sexual orientation.

3. Procedure

3.1 Responsibilities

3.1.1 Responsibilities of the Managing Director

The Managing Director has overall responsibility for ensuring compliance with this policy and associated data protection legislation.

The Managing Director also acts as the Data Protection Officer and takes full responsibility for the implementation of this policy.

In this capacity, the Managing Director will:

- monitor the implementation of this policy and supporting processes and assess their effectiveness in meeting obligations;
- ensure that all staff are aware of their responsibilities are accountable for managing data and records in areas of their control; and monitor compliance;
- implement improvements and corrective actions to minimise exposure where any weakness or potential non-compliance is identified;
- make adequate provision for necessary training and resources to ensure that confidentiality and data protection is managed effectively;
- formally authorise the release of records or data to a third party on an exceptional basis only;
- formally investigate and respond to any complaints regarding the use of personal information;
- If requested and permissible, provide a copy of an individuals personal data, along with details of how the information is being processed, to that individual within one month of a formal Subject Access Request;
- Maintain registration with the Information Commissioner's Office;
- Report data protection breaches that pose a risk to the 'rights and freedoms' of any individual to the Information Commissioner's Office.

The Managing Director also personally delivers confidentiality and data protection training during the induction program for new members of staff. The training stresses the importance effective document, records and data management, along with the necessary arrangements to protect personal information.

3.1.2 Responsibilities of the Headteacher

The Headteacher has primary responsibility for the implementation of our confidentiality and data protection policy and practices and for monitoring their effective implementation on a day-to-day basis. The Head teacher therefore:

- ensured sufficient staff are adequately trained in our confidentiality and data protection policy, related procedures, systems and make arrangements to inform staff of relevant data protection practices;
- ensure staff are competent in the tasks they are undertaking involving personal data and do not behave in a way that could lead to misuse or loss of information or unauthorised disclosure;
- log and report any non-compliance or deviation from this policy to the Managing Director.

APPROVED
This document is not approved for use
Issue/Date 2.1/(02/09/23)
Authentication 419228
Asset Identity POL00108

3.1.3 Responsibilities of all Staff

All staff are responsible for making sure that they are aware of, and comply with, confidentiality and data protection policies and procedures.

Similarly, all staff ensure that confidential data and personal information is stored and processed strictly in accordance with this policy and supporting procedures, while taking all reasonable steps to ensure that data and records are protected from loss, damage/corruption, misuse or unauthorised access or distribution.

Staff are required to raise queries with the headteacher and/or managing director regarding the use and storage of personal data if they are unsure regarding the legitimate and lawful use of this information.

Staff are required to report any concerns or non-conformities regarding implementation of this policy immediately, including potential or actual breaches of data protection, to the Headteacher and/or Managing Director.

Staff also take reasonable steps to ensure personal data and records for which they have responsibility, are accurate, up to date and adequate for the intended purpose.

Staff are not permitted, under any circumstances, to make unauthorised copies of personal data or records, including paper, electronic or photographic reproductions, etc.

In addition staff must never divulge information about the Robert Holme Academy, its pupils, staff or other stakeholders to unverified and illegitimate third parties, such as responding to unsolicited phone calls, emails, etc.

Staff must ensure computer systems and laptops containing personal data are password protected to prevent unauthorised access. Passwords must be at least 9 characters in length and must include a combination of alphanumeric and special characters. Passwords must be changed or a regular basis and must not be written down or shared with others. Computer systems and laptops containing personal data must be screen locked if they are to be left unattended at any time.

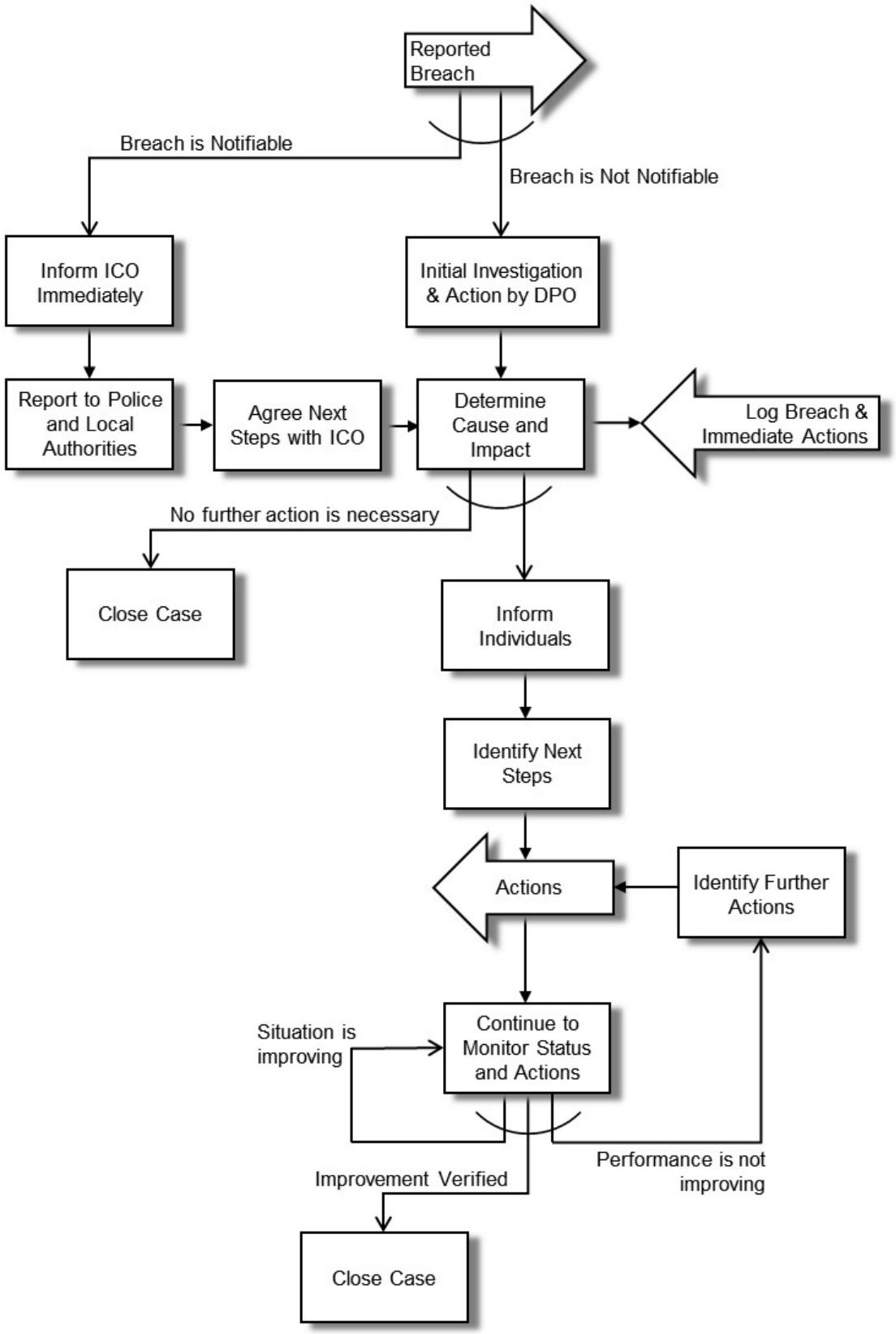
Staff must take all reasonable steps to avoid the introduction of viruses and prevent cyber attacks on our systems.

3.1.4 Responsibility of all Students

All students are also expected to comply with the our rules and, while students are not expected to know or appreciate the details and complexities of confidentiality and data protection, they are expected to understand and the principles and take appropriate precautions to protect themselves and others from risk and misuse of personal information.

Students are not permitted access, and must not attempt to gain access, to secure areas or systems where personal information is stored.

3.2 Process



APPROVED
This document is not approved for use
Issue/Date 2.1/(02/09/23)
Authentication 419228
Asset Identity POL00108

3.3 Reporting Data Protection Breaches

All privacy and/or data protection breaches are reported to and investigated by the Data Protection Officer.

Potential privacy and data protection breachs include, but are not limited to:

- virus or cyber attack;
- stolen or unauthorised release of personal information;
- unauthorised duplication of personal information, records or data;
- unauthorised disclosure of personal information or data;
- destruction or loss of personal information, records or data;
- non-compliance with privacy and data protection policy and procedure;
- loss or theft of computer, laptop or media containing personal information, records or data;
- unauthorised access to personal information, records, data or systems/facilities storing personal information, records, data (be they electronic or paper);
- any incident resulting in loss of access to stored information, including system failures, fire, flood, etc.;

The Data Protection Officer takes immediate action on receipt of a reported breach to determine the severity of the reported breach and it's impact. Privacy and data breaches are notifiable if they pose a risk to the 'rights and freedoms' of any individuals who may be impacted by the breach and are reported to the Information Commissioner's Office (ICO) within 72 hours of the reported breach.

Other breaches, including those that are not linked to personal information are formally recorded and processed in accordance with this policy, but are not reported to the Information commissioner's Office.

3.4 Notifiable Breaches

Notifiable breaches that are reported Information Commissioner's Office will include, as far as possible:

- the name and contact details of the Data Protection Officer;
- details of the breach that has occurred;
- details of the individuals that are or may be impacted by the breach;
- a description of the possible consequences of the breach;
- proposals of the immediate and longer term actions that are intended to address the breach and mitigate any possible adverse impact on the individuals impacted by the breach;

The Data Protection Officer reports as much information as is possible at this time, but further and more detailed investigation may be required to determine the full extent of a breach and it's possible impacts. In this instance, the report to the Information Commissioner's Office will include a plan of action and a proposed schedule for submitting any remaining information.

The Police will also be informed where criminal activity is evident or suspected. This includes, for example, a break-in at the premises or unauthorised access to school systems.

As far as possible, guidance on the actions to be taken will be determine in collaboration with the Information Commissioner's Office.

3.5 Determine Cause, Impact and Immediate Actions

All confidentiality and data breaches, be they notifiable to the Information Commissioner's Office or not, are investigated to determine the cause of the breach and the likely impact. Every effort is made to determine the individuals who are or could be impacted by the breach along with details of the information and data involved.

Immediate actions are completed as soon as possible following report of the breach. Particular attention is given to informing the individuals who are likely impacted by the breach to ensure they can take appropriate actions to mitigate any risk to themselves.

Details of the cause of the breach are also determined, including the those involved in the breach. As far as possible, data sources and audit trails including information such as access records, emails, and other evidence are preserved to permit a thorough investigation.

The Data Protection Officer may also notify relevant third parties who may be able to mitigate the impact of the breach on individuals. This may include the police, credit card company, insurers, banks, etc.

This information is formally documented and logged in a report prepared by the Data Protection Officer. The report will include the immediate actions to be taken to contain the breach, while mitigating risks and issues arising from the breach while limiting the impact on the Robert Holme Academy and individuals. The report will also detail proposed corrective actions to prevent any possible re-occurrence.

3.6 Inform Individuals

All individuals who are, or may be, impacted by the breach are notified, in writing, as soon as possible following the breach. The communication includes details of the:

- nature of the breach;
- their personal information or data that is impacted by the breach;
- the actions being taken to address the breach;
- recommended actions that the individual should take.

Further communication is provided if ongoing investigations reveal additional facts about the breach, particularly if the breach is considered to be more widespread or wider in scope than initial investigations reveal.

3.7 Identify Next Steps

A plan is then established by the Data Protection Officer to implement the actions necessary to prevent any further breach. Every action is assigned a responsible owner and a timescale for completion. Actions may involve a number of possible short-term and long-term activities. These may include:

- adjustment to policy, procedure and working practices;
- training and briefing staff;
- modification of systems, software, access controls, etc.

All actions arsing from the breach are formally documented. Each action includes a description of how the effectiveness of the action will be tracked to facilitate ongoing monitoring.

3.8 Monitor Status and Actions

The status of actions arising from the breach are reviewed and tracked to closure. Reviews are undertaken not less than once per calendar month, but may be more frequent depending on the priority of the action. Reviews involve the Data Protection Officer, Headteacher and owner of the action(s) along with other stake-holders, as required.

The impact and effectiveness of actions are also closely monitored as part of the regular review. Further actions are established if performance is judged not to be improving.

3.9 Close

The corrective action plan and corresponding actions are closed once they are verified as completed. The corrective action plan and supporting documentation is then removed from circulation.

4 References

This policy has been developed in line with the following legislation and associated guidance.

1. The Data Protection Act 2018, available at: https://www.gov.uk/data-protection
2. Information Commissioner's Office Guidance for Personal Data Breaches, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches