GDPR Breach Management Policy

Developed from Oldham Council Policy – January 2019, Reviewed Sept 2020

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, confidentiality, resilience and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from, other organisations and that this needs to be in accordance with the law.

1.2. This policy sets out the breach management policy obligations and accountability to which we are fully committed.

2. Scope

2.1. In order to fulfil our statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime data about living people, eg,

- Pupils and their families
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- Governors

2.2. This policy covers all aspects of handling personal data breaches, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR).

3. Policy

3.1. Data Protection Officer (DPO): We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

Data Protection Officer

Barbara Mulvihill

LA Data Protection Officer on behalf of Burnley Brow Community School:

West Street

Oldham OL1 1UT

Email: DPO@oldham.gov.uk

Tel: 0161 770 1311

3.2. What is an information security incident?

The definition of an 'information security incident' is an adverse event that has caused or has the potential to cause damage to our information assets, reputation and / or personnel or to people or organisations whose information we hold. Information security incident management is concerned with individual privacy intrusion, compromise and misuse of information and information resources, and the continuity of business processes and critical information systems.

Security incidents can be categorised according to the following:

- Confidentiality - where there is an unauthorised or accidental disclosure of, or access to, school information.
- Availability - where there is an accidental or unauthorised loss of access to, or destruction of, school information.
- Integrity - where there is an unauthorised or accidental alteration of school information

An information security incident includes, but is not restricted to, the following:

- the destruction, loss or theft of data or information – personal data and business
- the unauthorised disclosure or transfer of data or information to those who are not entitled to receive that information

Cyber security incidents are also captured within the definition of an information security incident. A cyber incident is a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems, as defined by the National Cyber Security Centre.

A cyber security incident includes, but is not restricted to, the following:

- attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- changes to information or data or system hardware, firmware, or software characteristics without our knowledge, instruction, or consent
- unwanted disruption or denial of service to a system that contains information
- the unauthorised use of a system for the processing or storage of data by any person
- malicious disruption and/or denial of service

For the purposes of this policy all incidents whether cyber or otherwise will be classified as information security incidents.
Examples of some of the more common forms of information security incidents are provided in Appendix 1.

3.3. Handling information security incidents

Information security incidents need to be reported at the earliest possible stage to Helen Atkinson-Smith as they need to be risk assessed by the school. This initial assessment should identify the level of risk attached to the incident and determine the appropriate mitigating actions that need to be implemented to manage that risk. Advice on the risk assessment of incidents can be obtained from the Local Authority DPO, Barbara Mulvihill.

It is vital for Helen Atkinson-Smith to be provided with as much information as possible from where the incident has originated.
Security incidents involving IT equipment or IT systems, e.g. suspected virus or member of staff responding to phishing email, must in the first instance be reported to Helen Atkinson-Smith who will carry out the appropriate action.
An evaluation / risk assessment must take place to identify any immediate action necessary to limit damage from the security incident and recover any losses.
Action may also be necessary to prevent another incident with similar circumstances while any investigation is taking place. This may include action taken to:

- establish and analyse the root cause(s)
- prevent any further unauthorised access
- secure any affected buildings, e.g. changing locks, access codes etc.
- recover any equipment or physical information
- restore lost or damaged data by using backups
- prevent a further security incident relating to the same information (e.g. an attempt to use stolen data to access accounts or services)

If an incident involves a data processor contracted to provide services on our behalf, it may be quicker for them to carry out the initial assessment themselves. However, it is important to bear in mind we may be responsible in law for the actions or omissions of a data processor and the contractor.

Reports on any information breach, including the type of breach, the investigation and any actions can be recorded on the 'Notification of Data Security Breach' template provided by the LA.

3.4. Incidents involving personal data

3.4.1. The General Data Protection Regulations (GDPR) applies to personal data. Personal data means any information relating to a person who can directly or indirectly be identified from the data.

Identifiers which could constitute personal data can include a name, identification number, location data or online identifier.

3.4.2. It must be noted that in the instance of a security incident involving personal data that reaches certain thresholds, the Information Commissioners Office (ICO), as the relevant supervisory authority, must be advised within 72 hours after becoming aware of it. By aware, we mean reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This brief period allows for some investigation, to gather evidence and to assess risk before we may have to notify. It is important to notify school within 12 hours to allow for the incident to be considered against notification criteria.

In the event of an incident involving personal data and an external data processor, where we can evidence seeking appropriate assurances from the contractor, the contractor could be liable for enforcement action from the ICO. To the extent this is provided for in an indemnity clause and / or other contract terms. For this reason, we must retain control over all decision making concerning security incident notification and the strengthening of technical and organisational security measures, including future contractual requirements.

3.4.3. The management and investigation of incidents involving data shared with or by the school will require a collaborative approach with relevant data sharing partners to learn lessons, strengthen data sharing arrangements and the management and assessment of adverse impacts.

The investigation may involve the following:

- Headteacher and other school staff
- Governing body
- The council, if appropriate
- Legal Services, if appropriate
- Risk and Insurance
- Any other relevant parties

Depending on the type and seriousness of the incident the employee/s may be suspended from the work place.

3.4.4. Security incidents if not acted on quickly, can cause data loss which in turn can lead to:

Service users

- physical harm
- mental anguish / distress
- financial loss
- identity theft

School and/or the council

- loss of public confidence / trust
- damage to reputation
- potential legal action
- financial penalties up to **€20 million** where personal data is involved
- administration fine of **€10 million** where the ICO or service users are not notified even though requirements to notify are met

3.4.5. Any identified weaknesses or vulnerabilities must be accurately assessed in order to mitigate the ongoing risks to information. In order to make an assessment, the following factors will be considered:

- type of data involved
- number of people that could be affected
- impact on individuals
- protections in place, e.g. encryption
- likelihood of the identified risk
- reputational risk to the organisation
- potential risks to public health or safety

3.4.6. Depending on the incident there may be legal, contractual or sector specific requirements to notify various parties. This may assist in security improvements and implementation, as well as risk mitigation.

The following parties may need to be notified following an information security incident:

Information Commissioner's Office (ICO)

- Does the incident involve personal data?
- Does the type and extent of the incident trigger notification?

Individuals

- Notification to the data subjects involved may be required where there is a risk to their rights and freedoms

Other Agencies (not an exhaustive list)

- National Cyber Security Centre
- Her Majesty's Revenue and Customs (HMRC)
- Bank or credit card companies
- Trade Unions
- Police
- DfE

Notification to any parties will be determined and agreed by the governing body/Headteacher as part of the evaluation of an incident.

It may also be necessary to follow the disciplinary procedure for any employee(s) involved in an information security incident.

3.5. Monitoring of information security incidents

All information security incidents are logged, referenced, risk assessed and tracked by Helen Atkinson-Smith and other delegated school staff with assistance from the LA where required.

This includes ensuring agreed mitigating actions have been implemented. Incidents are reviewed after closure to ensure that agreed preventative actions have been put in place Investigation reports must be signed off by the Headteacher and reports of incidents presented to the Governing Board on a regular basis.
The above includes any incidents that may have been reported to other agencies such as the Information Commissioner's Office, DfES etc.

4. Assessment and Monitoring

4.1. An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

Commented [BM1]: This would be good practice and help you demonstrate that you comply with the legislation and in particular the accountability principle, ie, where the onus is on the data controller to actively evidence compliance. Feel free to amend this section as suits your environment

4.2. Reports will be submitted to the Board of Governors.

5. Responsibilities and Approvals

5.1. **Governing Body**:

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. **Headteacher**:

The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

5.3. **Data Protection Officer**:

The Data Protection Officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

5.4. **Governors/Employees**:

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.

Appendix 1

Examples of common information security incidents are listed below. It should be noted that this list is not exhaustive.

- Inadvertently disclosing or giving personal information to someone who should not have access to it - verbally, in writing or electronically
- Sending an email containing personal information to the wrong email address
- Sending documents / paperwork containing personal information to the wrong address
- Theft / loss of a paper file containing personal information
- Theft / loss of any of our computer equipment
- Acting on an unsolicited email which requires you to enter personal data, e.g. username and password
- Unknown people asking for information which could gain them access to school data, e.g. a password or details of a third party
- Use of unapproved or unlicensed software on our equipment
- Computer infected by a virus or other malware
- Accessing a computer database using someone else's user id and password
- Writing down your password and leaving it on display / somewhere easy to find
- Printing or copying confidential information and not storing it correctly or confidentially
- Permanent loss of or accidental destruction to personal information
- Not complying with an individual's request to see information relating to them held by us
- Attempts to gain unauthorised access to a system and/or to data.
- Malicious disruption and/or denial of service.
- Unauthorised reversal of pseudonymised information