DATA BREACH POLICY

Date policy reviewed:	9 September 2024
Date of next review:	9 September 2026
Person(s) responsible for review:	SLT (DFO)

Policy Statement

The Manor holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a personal data breach. In the unlikely event of a personal data breach, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This data breach policy applies to all personal and sensitive data held by The Manor. It also includes a data breach procedure which applies to all School staff including volunteers, contractors and governors which are collectively referred to as 'staff'.

Purpose

This policy sets out the course of action to be followed by all staff at The Manor if a personal data breach takes place.

Legal Context

Data security is a cornerstone of the EU General Data Protection Regulation (GDPR). The sixth data protection principle – the integrity and confidentiality principle – requires The Manor to take appropriate technical and organisational measures to process personal data in a manner that ensures appropriate security including protection against:

- Unauthorised or unlawful processing; and
- Accidental loss, destruction or damage.

Types of Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. GDPR defines it as *"a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data"*. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, and this unavailability has a significant negative effect on individuals.

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Common examples of breaches experienced regularly at schools include: misdirected emails or post; insecure disposal of documents; equipment failure; failure to redact names in sharing information (e.g. when responding to a subject access request); or simply leaving documents or unencrypted devices unattended. Schools are also regularly subject to deliberate attacks on IT systems, such as hacking, viruses or phishing scams, e.g. emails advising fee-payers of “new” bank details.

Breach Procedure

It is important to draw a distinction between an obviously serious breach that triggers a crisis plan (involving potential roles for IT, legal and PR advisers) and a more minor breach that will be dealt with as a matter of policy and record. This distinction will become apparent as the School follows the below personal data breach procedure.

Step One: Notify the Head

The person who discovers/receives a report of a personal data breach must immediately inform the Head or, in his absence, the DFO. If the breach occurs or is discovered outside normal working hours, this person should nevertheless take all practical steps possible to inform the Head or nominated representative as soon as possible.

Step Two: Initial Assessment, Containment and Recovery

Within the first few hours of being notified of a breach, the Head (or nominated representative) must ascertain how long the breach has been taking place, what data was involved and how far it has progressed.

The Head (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant staff, so that they are prepared for any potentially inappropriate enquiries (‘phishing’) for further information on the individual or individuals concerned.

c. A group email to all school staff.

d. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details (if possible) and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Head (or nominated representative).
e. Contacting the Director of Admissions, Communications and marketing so that they can be prepared to handle any press enquiries.
f. The use of back-ups to restore lost, damaged or stolen data.
g. If bank details have been lost or stolen, consider contacting banks directly for advice on preventing fraudulent use.
h. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Other potentially appropriate steps include shutting down a system, or alerting relevant staff, such as the IT service provider Manager, if they may be able to assist. The Manor may also contact the Royal Mail, courier or other contractors if they have been involved and/or can assist.

Step Three: Ongoing Assessment of Risk and Mitigation

In most cases, the next stage would be for the Head (or nominated representative) to fully assess the breach as a matter of urgency. The Head (or nominated representative) should ascertain whose data was involved in the breach, the potential impact on the individuals and what further steps need to be taken to remedy the situation. The assessment should consider:

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

The steps that may need to be taken at this stage include informing:

a. The police or cyber fraud unit immediately where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future;
b. The Chair of Governors as soon as possible; and
c. The School's insurers in accordance with the insurance policy, e.g. where there is major loss, criminality or the potential for legal claims.

A clear record should be made of the nature of the breach and the actions taken to mitigate it.

The assessment should be completed as a matter of urgency and, wherever possible, within 72 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be carried out once the matter has been resolved.

Step Four: Notifying the ICO and Affected Individuals

Notifying the ICO (within 72 hours)

GDPR introduces a mandatory data breach reporting regime, however, notification to the ICO is not required for all data breaches. For instance, not every temporary system outage or loss of an encrypted device needs to be reported. Every incident should be considered on a case by case basis. The Head (or nominated representative) should, after seeking expert or legal advice, decide whether the ICO should be notified of the breach.

That said, the School may have already notified the ICO – perhaps on an 'interim' basis - as part of the initial assessment and containment of the breach under step 2 above. However, the breach can also be reported after an investigation has taken place under step 3 as long as it is within 72 hours of being aware of the breach.

Should the School notify the ICO?

GDPR states that a personal data breach must be reported *"…unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.*"

In other words, if it is likely that there will be a risk to individuals then The Manor must report it and this involves a focus on the potential negative consequences for individuals. A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some breaches will not lead to risks beyond possible inconvenience whilst others may significantly affect individuals whose personal data has been compromised. The Manor will assess this in relation to each breach.

How to notify the ICO

If a decision is made to notify the ICO, The Manor must report the breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it, even if it is a preliminary or interim notification. If the School takes longer than this, it must give the ICO reasons for the delay.

Where possible, the ICO notification should include a description of how and when the breach occurred, what data was involved and how many individuals are affected. The School should include details of what it has already done to mitigate the risks posed by the breach, i.e. the action taken under steps 2 and 3 above.

Breaches can be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Alternatively, the School may use the breach self-reporting form, which can be found on the ICO's website, and it can be emailed to casework@ico.org.uk.

If the School does not notify the ICO

If the School decides not to notify the ICO, it must still record that decision and the reasons for it.

Notifying Affected Individuals

Should the School notify affected individuals?

GDPR states that organisations, including The Manor, must notify affected individuals when the breach is "*likely to result in a high risk to the rights and freedoms of natural persons*".

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The Manor will assess both the seriousness of the impact (actual or potential) on individuals as a result of the breach and the likelihood of it happening. Where there is a high risk The Manor will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. The Manor will inform individuals if it would help them take steps to protect themselves from the effects of a breach.

How to notify affected individuals

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the School must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

When notifying individuals, The Manor will follow ICO guidance and describe, in clear and plain language, the nature of the personal data breach, and:

- the name and contact details of The Manor's contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Where appropriate, The Manor will describe to affected individuals what they can do to protect themselves (e.g. provide fraud or password advice) and what The Manor can do to help them. The Manor will also give affected individuals the opportunity to make a formal complaint to the School.

If the School does not notify affected individuals

If the School decides not to notify individuals, it will record that decision and the reasons for it. The School may still notify the ICO of the breach as the threshold for notifying the ICO is a lower one.

Step Five: Ongoing Evaluation, Monitoring and Remediation

The Head will continue to monitor and assess the possible consequences (even if it appears to be contained). If new information becomes available, the ICO and/or those affected should be updated. The ICO and/or those affected may also need to be informed of what The Manor is doing to remediate and improve practice.

The Head (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next SLT meeting for discussion. It should be compared with any previous breaches and any wider trends should be identified. If systemic or ongoing problems are apparent, then an action plan will be drawn up to put these right, which may include staff training and a review of this policy and/or other policies. This action plan will be reviewed regularly to ensure that it is implemented.

Disciplinary action

If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

Notifying the Charity Commission

The Manor is registered as a charity so any data breach that is reported to the ICO is also likely to result in the School being required to make a separate serious incident report to the Charity Commission. The report should be made as soon as is reasonably possible after the breach occurs or immediately after The Manor becomes aware of it. The School will seek advice from its legal advisers and consider the latest Charity Commission guidance on reporting serious incidents before deciding whether and how to report.

Advice and Assistance

The DFO is responsible for data protection compliance within the School. If you have any questions or comments about the content of this policy, or if you need further information, you should contact the DFO in person or by email: bursar@manorprep.org

Review of this Policy

This policy (including the breach procedure) may need to be reviewed after a breach or following legislative changes, new case law or guidance, or when the School's related data protection policies are reviewed.