Data Breach Policy

If you require this document in an alternative format please contact

office@tssmat.staffs.sch.uk **or 01543 472245**

Last review date:	September 2018
Next Review date:	September 2019
Review Cycle:	Annually
Statutory Policy:	Yes
Publication:	Website. SharePoint/Policies

Data Breach Procedures

Definition of a Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of 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. TSSMAT understands that a personal data breach isn't only about loss or theft of personal data. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

Personal data breaches can include, but are not limited to:

- 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.

Recognising a Data Breach

All staff will receive annual training on recognising data breaches, in addition to input at Induction.

All staff **<u>are required</u>** to report a data breach if witnessed or found immediately to the DPO and their relevant Headteacher, using the TSSMAT Data Breach Register. The DPO or Headteacher will inform the Chief Executive Officer, who will inform the relevant Director(s).

It is the notifying member of staff's responsibility to ensure the DPO and/or Headteacher are aware of the data breach, if they are not available, staff must contact another Headteacher and/or the Chief Executive Officer to ensure that a relevant person is aware of the breach, and has taken responsibility for co-ordinating action.

If action can be taken by staff immediately to correct or halt the data breach, this should be done. All actions should be noted on the TSSMAT Data Breach Register.

Response to a Data Breach

The Data Protection Officer (DPO) for TSSMAT is the Trust Administrator.

The DPO will be notified of all data breaches, internally and externally, via the TSSMAT Data Breach Report Form. The DPO's role is to co-ordinate the response to the breach, ensure corrective action is taken, and relevant bodies/individuals are notified if appropriate. If the DPO is not available, this role will fall to the Headteacher of the school the breach is relevant to, or the Chief Executive Officer if the breach concerns the MAT.

On receipt of the TSSMAT Data Breach Report Form, the DPO will ensure the relevant Headteacher, and the Chief Executive Officer are aware of the breach. The Chief Executive Officer will ensure the relevant Director(s) are aware of the breach.

The DPO will carry out an investigation into the breach using the Data Breach Investigation Report Form. The DPO will document the facts relating to the breach, its effects and the remedial action taken when and by whom.

The DPO will be responsible for informing the ICO or other relevant data protection agency (See Notifying the ICO), and affected individuals. The DPO is responsible for keeping the ICO/other DPA up to date as more information is gathered.

A report on data breaches will be presented to the Board of Directors at each meeting.

Records of data breaches will be kept in line with reports to the Board of Directors for 7 years.

Notifying the ICO or relevant International data protection agency about a Data Breach

If the ICO or other relevant data protection agency require notification, this will be done within 72 hours of TSSMAT becoming aware of the breach, even if full information is not available. To notify the ICO of a personal data breach, the DPO will use the ICO pages on reporting a breach.

TSSMAT will ensure the following information is provided, as soon as known, when notifying of a breach:

- a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other 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, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Notifying affected individuals of a Data Breach

If a breach has occurred, TSSMAT will inform those concerned directly and without undue delay, if the breach has or may result in severe risk to individuals or companies.

TSSMAT will ensure the following information is provided, as soon as known, when notifying affected individuals of a breach:

- the name and contact details of the TSSMAT data protection officer, or other 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.
- As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

This procedure is based on guidance on personal data breaches produced by the ICO.
Please see the Data Breach Procedure for more information

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Headteacher, and CEO. The Chair of Directors may also be notified.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's M Drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and

when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on M/Data Protection
- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Media Plan

If necessary, a media plan will be developed by the CEO and Chair of Directors. This will include nominated members of staff who are able to speak to the Media, development of key messages, and a timetable for updated information to be released.