General Data Protection Regulation Compliance Monitoring Procedure

If you require this document in an alternative format please contact office@tssmat.staffs.sch.uk or 01543 472245

Last review date:	December 2018
Next Review date:	December 2021
Review Cycle:	3 Years
Statutory Policy:	No
Publication:	Website. SharePoint/Policies

1. Purpose

To ensure that the organisation's compliance with the General Data Protection Regulation (GDPR) is monitored properly for adequacy and effectiveness, by setting out the system for a controlled method of raising and processing corrective and preventive action following the identification of a non-conformance.

2. Scope

This procedure applies to all areas of the organisation where personal data and/or special category data is processed. This includes the processing operations carried out by Board members, the Senior Leadership Team, and all employees and workers.

3. Guiding Principles

Legal compliance – the organisation is committed to ensuring the privacy and security of the personal data and special category data it processes and to meet its legal obligations as set out in the GDPR.

Consistency – this procedure sets out how compliance with the organisation's policies and working practices will be monitored to achieve transparency and consistency in approach.

Efficient and effective – the monitoring of technical and organisational measures is essential to understand whether the organisation's working practices are effective in keeping data secure and private and efficient in meeting operational need.

4. Accountabilities and Responsibilities

The data controller is ultimately accountable for ensuring compliance with the GDPR. The data controller is responsible for ensuring that appropriate and proportionate technical and organisation measures are implemented to achieve compliance. The Senior Leadership Team will undertake a review of the measures for data protection (including cyber security) on an annual basis.

The Data Protection Officer (DPO) will be responsible for facilitating compliance with the GDPR, undertaking monitoring activity to an agreed plan and reporting the findings to the Senior Leadership Team.

All employees and workers are responsible for cooperating with the DPO during monitoring visits and engaging in the process.

The manager responsible for the area of the organisation being monitored is responsible for ensuring that the findings and agreed recommendations from the monitoring visit are implemented and that agreed corrective or preventive action is taken within the specified timescale.

5. Programme of Monitoring Visits

Monitoring visits will be carried out in accordance with the organisation's GDPR Annual Monitoring Plan. The plan is determined by the Senior Leadership Team in

discussion with the DPO at the end of each academic year in readiness for the next year. Visits are planned throughout the year assessing and reviewing all the organisation's technical and organisational measures over time.

The visits are led by the DPO. The DPO will arrange the date of the monitoring visit with the manager of the area to be monitored. The DPO will remind the manager of the audit 1 week prior to the visit. A monitoring visit should be given priority so it occurs on the planned date.

6. Conducting Monitoring Visits

1. At the start of the monitoring visit, the DPO will meet with the manager (or nominated representative) to explain the scope of the visit and the process that is to be followed.

2. The DPO will check any corrective action from the previous monitoring visit.

3. The DPO will conduct the monitoring visit (see Appendix A – Guidance for Conducting Monitoring Visits) reviewing and recording evidence against the areas for monitoring. The detail of this will be recorded on the GDPR Monitoring Report form.

4. At the end of the monitoring visit, the DPO will conduct a closing meeting with the manager (or nominated representative). At this meeting, a brief overview will be given of the findings and any immediate concerns are discussed and action agreed. The manager is responsible for taking action for each non-conformance or observation found.

5. The DPO forwards the completed GDPR Monitoring Report to the Headteacher within 10 working days. The Headteacher is responsible for ensuring that any corrective action is taken within the agreed timeframes.

6. The Headteacher will agree a date within the term for the DPO to conduct a follow up visit to check that the agreed corrective action has been implemented.

7. Monitoring Visit Outcomes

A three-tier system is used to record conformance/non-conformances as follows:

Conformance – policies, procedures, processes and working practices are in place and are delivering data protection compliance.

Non-conformance – policies and/or procedures and/or processes and/or working practices are identified as a significant risk and data protection compliance will not be achieved. Action is required to ensure compliance.

Observation – policies and/or procedures and/or processes and/or working practices need to be improved to reduce the risk of non-compliance with data

protection requirements. Action is required to reduce the risk.

Corrective action is activity which corrects the immediate non-conformance, establishes the cause and takes steps to prevent a recurrence. When a non-conformance is identified in the course of a monitoring visit, the DPO will plan a follow up visit, one month after the event, to verify that the non-conformance has been corrected.

Preventive action aims to prevent the occurrence of problems, deviation and breaches. If during a monitoring visit, a policy, procedure or working practice is found to be either out of date, inaccurate or in need to review to reflect the requirements of the GDPR, this will be recorded by the DPO. The manager for that area will be responsible for reviewing the policy, procedure or working practice.

8. Review of Monitoring Process

On an annual basis, the Senior Leadership Team will review this monitoring process and the outcomes from monitoring visits (see Appendix B – Management Review), before setting the GDPR Annual Monitoring Plan for the next year. The outcomes of the management review should be reported by the CEO to Board of Directors to further demonstrate accountability and compliance with the GDPR.

Appendix A – Guidance for Conducting Monitoring Visits

1. Carry out the monitoring visit in accordance with the GDPR Annual Monitoring Plan and organisation's policy.

2. Check the status of previous non-conformances or observations raised; these should have been addressed and any corrective or preventative actions implemented and monitored by the manager following the previous visit.

3. Confirm with the manager that this has happened. If not, obtain a copy of the previous monitoring report and check that corrective action has been taken in all instances.

4. Note any specific instances of non-conformity with documented procedures and/or with the General Data Protection Regulation pertaining to the area.

   The monitoring report should include:

   - The scope of the visit (areas or functions to be checked and how);
   - Specific non-conformances or observations;
   - Suggested corrective action, where appropriate; and
   - Instances where existing documented procedures are not fully effective to meet the General Data Protection Regulation requirements

5. The monitoring report should be given as soon as completed to the manager and Headteacher.

6. Where non-conformity is detected with existing documented procedures, the document owner will be notified by the DPO and requested to conduct a review of the procedure within a month. Other stake holders involved in the process subject to review must be invited to assist in the review.

7. The monitoring report must be completed in full and a copy retained securely by the DPO.

Appendix B – Management Review

When reviewing the monitoring process, the Senior Leadership Team should consider the following areas:

Area for Review	Detail	Responsibility
Follow Up	Follow up of actions from previous management review.	All
Data Protection Policy	Review of the suitability and implementation of data protection policy/policies.	All
GDPR	Review of data and logs to confirm that technical and organisational measures are sufficient in ensuring compliance with the GDPR and to identify any improvements that be made or preventive action that can be taken.	DPO
Process Performance	Review of the monitoring process to ensure it performs satisfactorily and the outputs are effective in ensuring compliance.	All
Internal Monitoring	Review of the monitoring visit carried out. SLT to decide whether any significant changes need to be made to the monitoring system as a result of the findings.	DPO
Improvements and Preventive Action	Are there any other measures that could be taken to improve compliance with the GDPR? Have any appropriate preventive actions been identified?	All
Process Changes	Planned changes to the organisation's operations. Discussion on whether they could impact on the effectiveness of the existing monitoring system.	All
External Audits	Review of any audits related to GDPR carried out by external agencies. Do the findings/outcomes broadly agree with the internal monitoring process? Is any action required?	DPO
Any other Matters	For example, any changes in legislation or significant organisational change which may impact on compliance	All