SHREWSBURY COLLEGES GROUP

PERSONAL DATA BREACH NOTIFICATION PROCEDURE

Where there is a data breach within the College, it may be a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible. It is essential therefore that all data breaches, no matter how big or small, are reported to the DPO (DPO).

This Procedure should be read in conjunction with the Data Breach Policy and General Data Protection Policy. The Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you aware of the breadth of the concept of a data breach.

This Procedure should be followed by all staff. At all stages of this procedure, the Principal and DPO will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties, which process personal data on the College's behalf, that they have had a data breach which affects the College's personal data.

The procedure is set out below.

IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, however big or small, you must report this to the DPO immediately. The DPO is Mark Brown, Vice Principal – Quality, Apprenticeships & Information, and can be contacted at: 01743 653000, dpo@scg.ac.uk. Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the DPO.

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported.

False alarms or breaches that do not cause any harm to individuals, or the College, should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we can put in place.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether harm was caused. Please ensure that you report any breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

A data breach is confirmed when we have a reasonable degree of certainty that personal data has been being compromised. From this point, the time limit for notification to the ICO will commence.

When you report a data breach to the DPO, they will promptly investigate the breach to ascertain whether personal data has been compromised.

Should the DPO be unavailable the breach can be reported to the Head of Technical Services or the MIS Manager.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

SHREWSBURY COLLEGES GROUP

PERSONAL DATA BREACH NOTIFICATION PROCEDURE

ASSESSING A DATA BREACH

Once you have reported a breach and the DPO has investigated and decided that we are aware that a breach has occurred, they will log the breach in the Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is established, the DPO may notify the Principal; depending of the severity of the breach. Only Medium and High risk breaches will automatically be reported to the Principal. If necessary, the DPO will appoint a response team which may involve for example the HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the College and any individuals affected.

If the DPO and Principal consider that the breach is very serious, they will consider the impact on the College reputation and the effect it may have on the trust placed in us. The DPO and Principal will consider whether legal advice is needed.

THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.

FORMULATING A RECOVERY PLAN

The DPO will consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, the DPO may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, we must notify the breach to the ICO within **72 hours** of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The decision to notify the ICO will be based on the assessment of the DPO against the three key factors set out in the ICO Breach Notification guidance; **Potential Detriment, Volume of Personal Data, and Sensitivity of Data**.

The content of the notification will be drafted by the DPO and Principal in line with the Data Breach Policy, and the notification will be made by the DPO – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

SHREWSBURY COLLEGES GROUP

PERSONAL DATA BREACH NOTIFICATION PROCEDURE

NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by the DPO and Principal in line with the Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, explained in the Data Breach Policy, we may not need to notify the affected individuals. The DPO will decide whether this is the case. The decision to notify individuals will be based on the assessment of the DPO against the three key factors set out in the ICO Breach Notification guidance; **Potential Detriment, Volume of Personal Data, and Sensitivity of Data**.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Students
- Employees
- Parents/Guardians
- Employers
- Police, Insurers, Banks

The decision as to whether any third parties need to be notified will be made by the DPO and Principal. They will decide on the content of such notifications.

THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.

CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, the DPO will consider whether we need to update the ICO about the data breach.

THIS WILL BE CONSIDERED ON AN ONGOING BASIS.

EVALUATION AND RESPONSE
The key to preventing further incidents is to ensure that the College learns from previous incidents. It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. The DPO will carry out an evaluation as to the effectiveness of the College response to the data breach and document this in the Data Breach Register.