STOKE ON TRENT COLLEGE	**POLICY 52** **DATA BREACH POLICY**	

1.0 INTRODUCTION

This policy is designed to ensure Stoke on Trent College, its employees, agents and contractors can identify data breaches and meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth "personal data breach" or "data breach").

Data Protection Legislation means the Data Protection Act 2018[1] which incorporates the General Data Protection Regulation[2] (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003[3] and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time. On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025. The General Data Protection Regulation has been kept in UK law as the UK GDPR[4].

DEFINITIONS

a. Any reference to "Article" or "Articles" is a reference to an Article or Articles of the "GDPR".

b. The terms 'personal data', 'data subject', 'processing', 'pseudonymisation', 'controller', 'processor', 'recipient', 'third party', 'consent', 'personal data breach', have the meanings set out in Article 4 of the GDPR.

c. "Security incident" means an incident in which the security of personal data may have been compromised but no risk is identified in respect of the rights and freedoms of data subjects. Security incident in the context of this policy may also be used to define an event or action which may compromise the confidentiality, integrity or availability of systems or data, where such event or action does not presently amount to a reportable data breach.

2.0 DEFINITION OF A PERSONAL DATA BREACH

A personal data breach is defined within the Data Protection Legislation as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[2] https://gdpr-info.eu/
[3] https://www.legislation.gov.uk/uksi/2003/2426/contents
[4] https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/

The notification requirements associated with data breaches rest on the level of risk to the rights and freedoms of data subjects arising from the breach. Unless a personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned data subjects, it is to be reported to the ICO or relevant supervisory authority. Where such data breaches are likely to result in a high risk to the rights and freedoms of the concerned data subjects, the affected data subjects are to be informed in addition to the supervisory authority.

The Data Protection Legislation further stipulates that where notification of the supervisory authority is required, this should take place within 72 hours of the controller becoming aware of the personal data breach. In the case of breaches which pose a high risk to data subjects, the additional requirement to notify data subjects must be done as soon as possible and without undue delay.

In light of these requirements, this policy focuses on the responsibilities of all employees, agents and contractors associated with the Stoke on Trent College in internally reporting breaches and the external notification requirements.

3.0 RESPONSIBLE PERSONS

The Directors of the organisation have responsibility for ensuring that any privacy risks are managed.

All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant in order to ensure breaches are identified, reported and managed in a timely manner.

All staff are responsible for reporting mistakes, suspected or actual data breaches at any given time. They must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and could lead to disciplinary action.

4.0 BREACH RESPONSE PROCESS

a) Identify the breach

Personal data breaches could include:

- access by an unauthorised third party
- deliberate or accidental actions by a controller or processor or their employees, agents or contractors

- human error affected personal data
- sending personal data to an unauthorised recipient
- network intrusions
- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- alteration of personal data without permission
- loss of availability of personal data

b) Report the Breach

When reporting a security incident or personal data breach, suspected or actual, the reporter is obliged to disclose all information within their knowledge using the **Breach Report Form** annexed to this Policy (Annex 1). This must be submitted to the DPO immediately. The DPO will analyse the form, update the Data Breach Log, investigate the breach and ascertain whether any immediate corrective, containment or escalation actions are required.

c) Investigate the Breach

Stoke on Trent College aims to complete a preliminary investigation of all reported incidents without undue delay, with an aim to establish its awareness of a personal data breach within the **first 24 hours** of internal detection.

From that point, there are **72 hours** within which to identify whether there is a risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place.

During the investigation, Stoke on Trent College aims to establish the following:

- The facts of the security incident
- The data or records concerned
- The value and sensitivity of the data or records concerned
- The type of breach suspected (confidentiality, availability, integrity)
- The number and identity of affected data subjects
- To identify and assess the ongoing risks (by carrying out a **Root Cause Analysis**) that may be associated with the breach. In particular, an assessment of;
    - potential adverse consequences for individuals
    - their likelihood, extent and seriousness
- Determining the level of risk will help define actions in attempting to mitigate those risks and Stoke on Trent College's notification responsibilities
- The measures required to contain the impact of the breach

d) Notify the Supervisory Authority

All personal data breaches which pose a risk to the rights and freedoms of data subjects must be reported to the Information Commission's Office (ICO) within 72 hours of becoming aware of a relevant breach.

Stoke on Trent College aims to ensure all such notifications are made within 72 hours of becoming aware of the personal data breach.

All notifications to the ICO must be made with the authorisation of an executive employee of Stoke on Trent College and will be made using the breach notification form[5] provided by the ICO after a self assessment of whether it can be reported online[6].

e) Notify the affected Data Subjects

Where a high risk to the rights and freedoms of data subjects is established in the Risk Assessment, Stoke on Trent College will inform data subjects of the personal data breach as soon as possible and without undue delay.

Communication to data subjects should include:

- The nature of the breach
- The name and contact details of the DPO or other contact person
- The likely consequence of the breach
- The measures taken or proposed to be taken by the controller to address the breach
- any recommended steps to be taken by the data subjects themselves e.g. changing passwords

Stoke on Trent College aims to notify data subjects of relevant personal data breaches directly unless it is impossible to do so, or it would involve a disproportionate effort, in which case the breach may be communicated by way of a public statement. All such communications must be authorised by an executive employee.

f) Notify Others

Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.

These could be police, other regulatory or supervisory authorities, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

[5] https://ico.org.uk/media/report-a-concern/forms/4019685/report-a-personal-data-breach-form.doc
[6] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

This list is not exhaustive.

5.0 ACCOUNTABILITY

All security incidents reported will be documented regardless of whether the breach was notifiable to the ICO. Stoke on Trent College will maintain a Data Breach register containing all reported incidents.

6.0 EVALUATION

The DPO will evaluate the effectiveness of Stoke on Trent College's response to the breach to learn and apply any lessons or remedies or recommendations in the light of findings or experience across the organisation.

7.0 APPROVAL

Approved by the College Executive Team

Signed: 

(Principal)

Endorsed by the College Corporation

Signed: 

(Chair)

STOKE ON TRENT COLLEGE	POLICY 52 **DATA BREACH POLICY**	

Annex 1

Please complete this form if you have detected or been advised of a data breach. It is imperative that you complete this form immediately upon detection and where possible, please advise your line manager of the suspected breach immediately.

Once completed, please email this form to dpo@stokecoll.ac.uk

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	
Brief description of how you became aware of the incident:	

Issued	Reviewed	Reviewed						
11.7.19	**6.12.22**	**15.01.24**						

Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	
Approximate number of affected records, if known:	
Any actions taken in response to the incident:	