South Gloucestershire and Stroud College & Academy Trust

Data Privacy & Protection Policy

Data Breach Notification code of practice and procedure

TABLE OF CONTENTS

1. *OVERVIEW*

The reputation and future growth of SGS (including South Gloucestershire and Stroud Group and the SGS Academy Trust) are dependent upon the way the organisation manages and

protects Personal Data. As an organisation that collects and uses Personal Data, we take seriously our obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The Group's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected.

All staff will receive a copy of this code of Practice when they start and may receive periodic revisions of this Code of Practice through Monday Memo or normal school communication channels. This Policy does not form part of any Personnel contract of employment and the Group reserves the right to change this Policy at any time. All Group Personnel are obliged to comply with this Policy at all times.

2. ABOUT THIS CODE

This Code of practice MUST be read in the context of the College or Academy Trust's Data Privacy & Protection Policy. The Group Executive Team also has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the Group deals with and records Personal Data breaches.

3. SCOPE

This Policy applies to all staff who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. DEFINITIONS

4.1. Staff - Any employee or contractor who has been authorised to access any of the Group's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the organisation.

4.2. Data Protection Laws - The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

4.3. Data Protection Officer - The Data Protection Officer is Gavin Murray and can be contacted at: DataPrivacy@sgscol.ac.uk

4.4. ICO - the Information Commissioner's Office, the UK's data protection regulator.

4.5. Personal Data - any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious

beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

4.6. *Special Categories of Personal Data - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.*

5. WHAT IS A PERSONAL DATA BREACH?

5.1. *The group takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. SGS Group also has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.*

5.2. *Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.*

5.3. *A Personal Data breach could include any of the following:*

5.3.1. *loss or theft of Personal Data or equipment that stores Personal Data;*

5.3.2. *loss or theft of Personal Data or equipment that stores Personal Data from a Group supplier (or individual organisation);*

5.3.3. *inappropriate access controls meaning unauthorised staff or others can access Personal Data;*

5.3.4. *any other unauthorised use of or access to Personal Data;*

5.3.5. *deleting Personal Data in error;*

5.3.6. *human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);*

5.3.7. *hacking attack;*

5.3.8. *infection by ransom ware or any other intrusion on our systems/network;*

5.3.9. 'blagging' offences where information is obtained by deceiving the organisation who holds it; or

5.3.10. destruction or damage to the integrity or accuracy of Personal Data.

5.4. A Personal Data breach can also include:

5.4.1. equipment or system failure that causes Personal Data to be temporarily unavailable;

5.4.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

5.4.3. inability to restore access to Personal Data, either on a temporary or permanent basis; or

5.4.4. loss of a decryption key where Personal Data has been encrypted because this means the Group cannot restore access to the Personal Data.

6. REPORTING A PERSONAL DATA BREACH

6.1. Staff must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not they think a breach has occurred or is likely to occur (this includes both false alarms and near misses). This allows Group to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and each institution within the Group.

6.2. If a Personal Data breach is discovered outside working hours, staff must notify the Group's Data Protection Officer as soon as possible.

6.3. Staff may be notified by a third party (e.g. a supplier that processes Personal Data on the Group's behalf) that they have had a breach that affects Group Personal Data. Any breach of this type must be notified to the Group's Data Protection Officer and the Group's Data Breach Notification Procedure shall apply to the breach.

7. MANAGING A PERSONAL DATA BREACH

7.1. There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

7.1.1. Containment and recovery

7.1.2. Assessment of on-going risk

7.1.3. Notification

7.1.4. Evaluation and response

7.2. At all stages of this Policy, the Data Protection Officer and managers will consider the need to seek external legal advice.

8. CONTAINMENT AND RECOVERY

8.1. An initial assessment of the Personal Data breach will be carried out by theData Protection Officer.

8.2. If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the Group' s Data Breach Register and no further action will be taken.

8.3. If the Data breach may impact on the rights and freedoms of the individuals affected then the Group will put together and implement a bespoke Data breach plan to address the breach concerned in accordance with the Group's Data Breach Notification Procedure. This will include consideration of:

8.3.1. whether there are any other people within the Group who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

8.3.2. what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

8.3.3. whether it is necessary to contact other third parties such as learners, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. Only the data Protection Officer is authorised to make notifications.

8.4. All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

8.5. The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

9. ASSESSMENT OF ONGOING RISK

As part of the Group's response to a Personal Data breach, once the breach has been contained the Group will consider the on-going risks to the Group, the constituent organisations within the Group and to any other party, caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the Group's Data Breach Notification Procedure.

10. *NOTIFICATION*

10.1. Under Data Protection Laws, the Group may have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

10.2. Any notification will be made by the Data Protection Officer following the Group's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

10.3. Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the Group becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore imperative that Group Personnel notify all Personal Data breaches to the Group in accordance with the Data Breach Notification Procedure immediately.

10.4. Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

10.5. Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the Group will decide whether to notify and who to notify in accordance with this code of practice.

10.6. Where the Personal Data breach relates to a temporary loss of availability of the Group's systems, the Group does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The Group does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with this code of practice.

10.7. In the case of complex breaches, the Group may need to carry out in-depth investigations. In these circumstances, the Group will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with this code of practice.

10.8. Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with this code of practice.

10.9. When the Group notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with this code of practice. Any notification to an individual should include details of the action the Group has taken in relation to containing the breach and protecting the individual. It should also give any

advice about what they can do to protect themselves from adverse consequences arising from the breach.

10.10. The Group may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with this code of practice and shall be made by the Data Protection Officer.

11. *EVALUATION AND RESPONSE*

11.1. It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the Group's response to it and the remedial action taken.

11.2. There will be an evaluation after any breach of the causes of the breach and the effectiveness of the Group's response to it. All such investigations shall be carried out in accordance with this code of practice and will be recorded on the Personal Data Breach Register.

11.3. Any remedial action such as changes to the Group's systems, policies or procedures will be implemented in accordance with this code of practice.

12. *PROCEDURE*

IDENTIFYING AND REPORTING A DATA BREACH
If you discover a data breach, however big or small (including false alarms and near misses), you must report this to our Data Protection Officer immediately by contacting DataPrivacy@sgscol.ac.uk providing as much information as is possible. A data breach could be as simple as you putting a letter in the wrong envelope— even the most minor data breaches ***must*** be reported. False alarms or even breaches that do not cause any harm to individuals or to the Group should nevertheless be reported as it will enable us to learn lessons on how we respond and the remedial action we 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 any harm was caused. Please ensure that you do report any data concerns, even if you are unsure whether or not it is a breach.**

BECOMING AWARE OF A DATA BREACH – INVESTIGATING
We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence. When you report a data breach to the Data Protection Officer it will be promptly investigated breach ascertain whether we are fully aware that a breach has occurred that

has led to personal data being compromised.
THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

ASSESSING A DATA BREACH

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

Once the level of severity is known, our Data Protection Officer will notify the Executive Management Team and the relevant Governing Body (being either the SGS College Further Education Corporation or the SGS Academy Trust Board). If necessary, we may appoint a response team which could involve for example our HR and IT services 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 our Data Protection Officer and the Executive Management team consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and Executive Management Team will consider whether to issue a press statement and will also consider whether legal advice is needed.

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

NOTIFYING A DATA BREACH TO THE ICO

If the breach is likely 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 content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy, and the notification will be made by our Data Protection Officer – 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.

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 our Data Protection Officer in line with our Data Breach Policy and in conjunction with 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 our Data Breach Policy, we may not need to notify the affected individuals. Our Data Protection Officer will decide whether this is the case.

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:

- Insurers
- Police
- Employees
- Learners/Pupils
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and Executive Management team. 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, our Data Protection Officer 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 we need to take to prevent a recurrence of the incident. Our Data Protection Officer and Executive Management team will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.

FORMULATING A RECOVERY PLAN

Our Data Protection Officer and Executive Management team will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer, the Head of HR or the Head of IT Services may interview 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.