Skinners' academy

Data Protection Policy

Principal	Shereka James
Person Responsible	Olu Alalade
Committee Responsible	Finance & General Purpose
Chair of F&GP Committee	David Fitzsimmons
Review Cycle	Annual
Governing Body Ratification	June 2023
Review Date	June 2024
Legal Framework	• UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 • Data Protection Act 2018 (DPA 2018) • It also reflects the ICO's code of practice for the use of surveillance cameras and personal information • In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. • In addition, this policy complies with our funding agreement and articles of association
Summary of changes from last version	See Appendix 2

Contents

1. Introduction

Skinners' Academy is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its obligations under the Data Protection Act 2018 (DPA). This policy sets out Skinners' Academy's commitment to data protection, and individual's rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, volunteers, and former employees, referred to as HR-related personal data, and likewise the personal data of pupils and their parents and explains how Skinners' Academy will hold and process the information we have about individuals.

This policy is non-contractual and may be amended at Skinners' Academy's absolute discretion.

Skinners' Academy has appointed Judicium Consulting Limited as its Data Protection Officer. The DPO's role is to inform and advise Skinners' Academy on its data protection obligations. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer at dataservices@judicium.com or at Judicium Consulting Limited, 72 Cannon Street, London, EC4N 6AE.

Day to day data protection matters will be handled by the Chief Financial Officer and the Human Resources Manager who are designated as Academy Data Champions. Both will coordinate all data protection matters with respective departments and line managers.

2. Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it. Skinners' Academy holds personal data in electronic and paper HR files, email systems, company intranet, security records and systems, timekeeping records, telephone recording and monitoring systems, CCTV and IT monitoring systems.

Personal data may be provided to Skinners' Academy by individuals through CV's and application forms, but also from third parties such as former employers, or may be created during the employment relationship (such as performance, training or absence records) or on its termination (such as references provided to prospective employers).

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. Some of this information may be collected in an anonymised format to monitor the effectiveness of equal opportunities policies. Where this is the case, it will not be considered to be personal data. However, where the data has not been anonymised, this will clearly be special category data and treated as such.

Details of any special category data Skinners' Academy collects, and processes will be explained in detail when collected.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings, which is collected to meet regulatory requirements.

"Processing" means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. It applies to a comprehensive range of activities including the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

"Data Champion" refers to the employees and DPO's first point of contact for data protection queries.

"Data Controller" means a person or organisation that determines the purposes and the means of processing of personal data.

"Data Processor" refers to person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

"Data Subject" refers to the identified or identifiable individual whose personal data is held or processed.

3. Data Protection Principles

Skinners' Academy processes HR-related personal data in accordance with the following data protection principles, which set out that all personal data shall be:

- processed lawfully, fairly and in a transparent manner
- collected and processed for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purposes of processing
- accurate and in date and any inaccurate data rectified or erased without delay
- only kept for the period of processing and no longer than is necessary
- processed in a way that ensures appropriate security.

In line with data protection principles Skinners' Academy will only process employee's personal data and special category data for the reasons notified to employees and in accordance with its obligations. Under the DPA, Skinners' Academy must have a specified lawful basis for processing an employee's personal data.

Skinners' Academy processes personal data where necessary to manage the employment relationship and the main lawful bases for processing individual's data are:

- to comply with its legal obligations (e.g. paying tax and National Insurance contributions)
- to fulfil the contract with the individual (e.g. to pay according to the rate agreed), and
- because it is necessary for Skinners' Academy's legitimate interests (e.g.to ensure Skinners' Academy can forward plan).

Where one of these reasons applies Skinners' Academy may process an individual's data without their consent. Individuals may choose not to give us certain data but they should be made aware that this may prevent Skinners' Academy from complying with its legal obligations and this may in turn affect their employment.

Where Skinners' Academy processes special categories of personal data or criminal records data it will be done where one of the lawful reasons applies and where either:

- the individual has given explicit consent
- processing is necessary under employment law
- processing is necessary to protect the individual's vital interests and the individual is incapable of giving explicit consent
- the individual has made the data public
- processing is necessary to do with a legal claim
- it is required for occupational medical reasons, or for the assessment of an individual's working capacity.

Where we plan to process special category data we will explain this, and set out the reasons, at the time. Special information where relevant will not be used to discriminate against individuals in any manner. Skinners' Academy will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

4. Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

Individuals, whether pupils, applicants, employees or former employees, have the right to review the information that the Company holds about them, with some exceptions. A subject access request can be made verbally or in writing, in a hard copy letter or transmitted electronically by email or text and may also be valid if submitted by means of social media. If an individual wishes to make a "subject access request" he or she can be requested to confirm the request in writing to the person nominated to monitor data protection, or to the Principal's PA and HR Manager. However, it is not compulsory for an individual to do so, nor can it be used as a means of extending the one-month time limit.

Skinners' Academy will usually respond within one month. If the request is complex the timescale for a response may be extended by up to two months. Where this is the case, Skinners' Academy will advise the individual within one month of receiving the request and explain why more time is needed.

No charge will usually be made for a response to a subject access request.

If anyone receives a subject access request from another member of staff, the request should immediately be forwarded to the person nominated to monitor data protection, or HR.

Other Rights

Individuals have a number of other rights in relation to their personal data:

- have the right to be told what personal data Skinners' Academy processes, how this processing takes place and on what basis

- have the right to receive a copy of their personal data, and in some circumstances have their personal data transferred to another data controller, usually within a month, and without any charge
- to rectify inaccurate data
- to ask Skinners' Academy to erase personal data where it is no longer necessary to process it for the purpose it was collected or where it should not have been collected in the first place
- to object to data processing where Skinners' Academy is relying on a legitimate interest to do so and the individual thinks that his or her rights and interests outweigh those of Skinners' Academy
- to be notified if there is a data security breach involving their data that may affect them
- have the right not to consent, or to later withdraw consent to processing where Skinners' Academy was relying on consent as the lawful reason to process personal data
- have the right to complain to the Information Commissioner. Contact details can be found on the website: www.ico.org.uk.

5. Data Security

Skinners' Academy takes the security of all personal data seriously. Skinners' Academy has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Access to individual's data is restricted to those users with a specific and legitimate business need for the data.

Where Skinners' Academy engages third parties to process personal data on its behalf, Skinners' Academy still retains responsibility for the secure and appropriate use of that data. Consequently, before an individual's data is transferred to any third party, Skinners' Academy will:

- Ensure that the third party has sufficient security measures in place to protect the processing of personal data
- Ensure any transfer of data is done securely, either by password protecting documents, or by transferring data via a secure collaborative portal
- Have in place a written contract establishing what personal data will be processed and for what purpose
- Ensure that a data processing agreement has been signed by both parties.

6. Impact Assessments

Some of the processing that Skinners' Academy carries out may result in risks to privacy. Where processing could result in a high risk to individual's rights and freedoms, Skinners' Academy will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

7. Data Breaches

If Skinners' Academy discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Skinners' Academy will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8. International Data Transfers

Skinners' Academy will not transfer personal data to countries outside the EEA.

9. Individual responsibilities

Employees are responsible for helping Skinners' Academy keep their personal data up to date. They should let Skinners' Academy know if data provided to Skinners' Academy changes, for example if an employee moves to a new house or changes his/her bank details.

Any employee who has access to personal data of other employees or clients/customers must familiarise themselves with this policy, including the data protection principles and comply with them.

Employees who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes,
- not to disclose data except to individuals (whether inside or outside Skinners' Academy) who have appropriate authorisation,
- to keep all data secure – whether on paper or electronically. For example, by complying with rules on computer access, including password protection, and secure file storage and destruction. Always lock electronic devices when not in use and keep paper-based personal data in locked cabinets. In keeping electronic data secure, ensure that multi factor authentication (MFA) is in use,
- not to remove personal data, or devices containing or that can be used to access personal data, from Skinners' Academy premises without permission and by adopting appropriate security measures (such as encryption or password protection) to secure the data and the device,
- not to store personal data on local drives or on personal devices that are used for work purposes,
- to securely destroy all copies of personal data they create, and
- to complete a data breach reporting form (see Appendix 1) and report data breaches of which they become aware to their line manager or Head of Department immediately. Line managers or Heads of Department should assess and determine if the breach poses a risk to the rights and freedoms of the affected staff and if so, report to the Data champions. Staff are required to complete a Data Protection training module annually.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Skinners' Academy's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

10. Training

Skinners' Academy will provide training to all employees about their data protection responsibilities as part of the induction process and at regular intervals thereafter. This needs to include awareness of any restrictions on personal use of Skinners' Academy's systems as detailed in the Skinners' Academy's IT policy.

Employees whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

11. Monitoring

Skinners' Academy monitors individual's use of Skinners' Academy's computer systems (including emails and the use of the internet on company computers and other devices) because it needs to do so to protect other employees and because of duties owed to suppliers and customers.

If any other monitoring is being considered, staff will be advised of this and given all the relevant information, including the lawful basis for processing the data, at the time such monitoring is put in place. In all cases, a Privacy Impact Assessment will be undertaken. Covert monitoring will only take place exceptionally and where the Privacy Impact Assessment has established that there is no less intrusive way to gather the information.

12. Photograph and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

We also require all key stakeholders, including students, to respect the privacy of others and ask them to refrain and be mindful of photographing others, and to consider context and nature of the photograph. We have in place Acceptable Use of the Internet Policy specific to students, which covers this in more detail.

APPENDIX 1: **Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the data champions must immediately notify the data protection officer (DPO) by using a dedicated email address - dataservices@judicium.com or at Judicium Consulting Limited, 72 Cannon Street, London, EC4N 6AE, using the Academy Data Breach Reporting Form as shown below.

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

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way) in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored securely on the Academy's computer systems.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 Academy Log of breaches as monitored by Data Champions.

The DPO and CFO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and CFO will meet regularly (termly) to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals:

- the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the Data Champion or Line Manager will ask the ICT department IT support to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Data Champion will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The Data Champion will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- Upon escalation, the DPO will carry out an internet search to check that the information has not been made public; if it has, the Academy will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the Data Champion will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach to consider include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked, and parents' financial details stolen.
- Hardcopy reports sent to the wrong pupils or families.

DATA BREACH ESCALATION PROCEDURE

- Skinners' Academy takes the security of personal data seriously.
- Its internal policies and controls are designed to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.
- Access to individual's data is restricted to those users with a specific and legitimate business need for the data.
- GDPR regulation requires that personal data breach posing a risk to the rights and freedoms of individuals are reported to the Information Commissioner within 72 hours.
- Where there has been a personal data breach, a Data Breach Reporting Form (see below) should be completed **immediately** by the staff member how has made the breach and submitted to their line manager or Head of Department.
- The line manager and/or Head of Department should assess and determine if the breach poses a risk to the rights and freedoms of the affected staff.
- If this is so, the Data Breach Reporting Form and detailed documentation is forwarded to the Academy Data Protection Champions; Olu Alalade - Chief Financial Officer and Lois Kates - HR Manager, within **24 hours**.
- The Data Protection Champions will log the data breach and forward to the Academy Data Protection Officer (DPO) - dataservices@judicium.com or at Judicium Consulting Limited, 72 Cannon Street, London, EC4N 6AE.
- The DPO then conducts an assessment and ensures that the data breach is reported to the Information Commissioner within 72 hours of discovery.

- If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Champions will tell the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

DATA BREACH REPORTING FORM

Report prepared by: **On behalf of:**

Today's Date:

		Data Breach Details
1	Summary of the event and circumstances	
2	Type and amount of personal data	
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	
5	Procedures / instructions in place to minimise risks to security of data	
6	Breach of procedure/policy by staff member	
7	Details of notification to affected data subject Has a complaint received from Data Subject?	
8	Details of Data Protection training provided:	

9	Procedure changes to reduce risks of future data loss	
10	Conclusion	

APPENDIX 2: **Table of substantive policy changes from June 2022**

Where	What
Page 8 – Section 9	Under Individual responsibilities, and bullet point 'to keep all data secure' introduced the need to ensure Multi Factor Authentication is in use to keep electronic data secure.