Data Protection Policy

Introduction

This Data Protection Policy has been reviewed and re-written to incorporate the provisions of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. This policy covers all personal data held by the Academy as the Data Controller.

We hold the personal data of Students, Parents and Staff. Personal Data is defined by the GDPR as:

> **Any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified directly or indirectly, in particular by name, identification number, location data, online identifier or one or more factors specific the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person**

We will abide by the provisions of the GDPR and the Data Protection Act 2018 and will seek to control the personal data we hold in a lawful, fair and transparent manner.
We will take all reasonable steps to ensure that partner organisations who process data on our behalf, also abide by the provisions of GDPR and the Data Protection Act 2018.
Whilst our Governing Body may delegate management and implementation of Data Protection to the Principal and Data Protection Officer, it remains the responsibility of the Governing Body to ensure compliance with GDPR and the Data Protection Act.
These procedures apply to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Aims

We aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors, and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance

These procedures meet the requirements of the GDPR and the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. In addition, these procedures comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. All our procedures are in line with the funding agreement and articles of association for Stanchester Academy.

Data Protection co-ordinator

Our named data protection co-ordinator is Gerry Stone IT Manager , his role is supported by Amy Joynes, Principal. The data protection co-ordinator is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Stanchester Academy, on behalf of the school, is registered as a data controller with the ICO and will renew this registration every five years, as legally required.

Privacy Notices

We have two privacy notices relevant to our school which are available to view on the school website. The privacy notice for parents outlines how we process pupil data and is displayed in the school Reception area.
The privacy notice for school staff is displayed in the M- Drive under policies.

Fair, Lawful and Transparent Processing

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that we can fulfil a contract with the individual, or the individual has asked us to take specific steps before entering into a contract.
- The data needs to be processed so that we can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that we, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
We offer online services to students, such as classroom learning apps, and where we intend to rely on consent as a basis for processing, we will get parental/carer consent (except for online counselling and preventive services). When we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Data Sharing

The efficient operation of the Academy requires that personal data is shared with a range of organisations, identified on the Privacy Notice. The Academy may share this data providing it is for activities in the public interest.
The Academy, as the Data Controller, has a legal obligation to ensure that organisations with whom it shares data also comply by the GDPR and the Data Protection Act 2018. External organisations who are processing the Academy's data will be required to provide formal reassurance which confirms their compliance with these regulations.

Data Accuracy and Destruction

We will take all reasonable steps to ensure that the data it holds is accurate. Students, Parents and Staff will be asked annually to confirm the accuracy of the data that is held. In addition, they will be reminded on the website and through newsletters and briefings to keep the Academy informed of changes to personal circumstances. Where it becomes known that personal data is inaccurate, this will be deleted immediately, and all reasonable efforts made to obtain the correct data.

The Academy will ensure that it reviews the data that it holds and will not keep that data longer than is required. The Academy will ensure that destruction of data is carried out by a licensed contractor and that appropriate records of the destruction are maintained.

Data Breaches

We will make all reasonable effort to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the attainment of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

Visitors

All visitors are asked to sign in on arrival to the school. The visitor sign-in system will not allow the personal information of other visitors to be viewed. To maintain confidentiality, the glass screen is only opened as necessary by the office staff. Visitors who wish to speak privately are given this option by the office staff.

Clear Screen Policy

In order to preserve the confidentiality of data held in school it is our policy that all members of staff should lock their PC screens when leaving it unattended. This can be achieved by pressing the CTRL+ALT+Delete keys simultaneously and then selecting the lock option.
When talking to parents, professionals or other members of staff who do not need access to the data the screen should be positioned so that it cannot be viewed or locked.

Encryption

All laptops that are taken off site are encrypted. If a laptop was to be mislaid or stolen this breach should be reported immediately to the data protection coordinator and ICT lead.

Passwords and Passcodes

All staff are issued with network, email, SIMS and relevant online or cloud-based software passwords. It is essential that passwords are not shared. It is not considered

good practice to write down passwords, however, should this be deemed necessary this information should be locked away securely when not in use.
Passwords should be at least eight characters long containing letters and numbers, when used to access school computers, laptops, printers and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Some teaching staff have been provided with an iPad. Every iPad must be secured using a six-figure passcode. IPads can be tracked and traced using the Apple software. If an iPad was lost or stolen it should be reported to the IT lead.

Removable Media

Staff should save work into the Office 365 'One Drive' folder linked to their email account. Within this account members of staff can choose whether this is a personal document or whether it is to be shared with other members of the school staff. Documents that are saved within One Drive can be sent electronically as a link or as an attached copy.
Staff have been issued with encrypted USB storage devices. These devices should be kept secure, and any loss should be reported to the IT lead and Data Protection co-ordinator.

Emails

As a school, we use Office 365 as our email system. All school correspondence will only be emailed to school provided email addresses, both for staff and governors. Passwords for emails must be kept securely. When emailing personal data about a child or member of staff initials should be used, as appropriate. Documents containing personal data should be password protected and the password for the document sent in a separate email.

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 Data Protection co-ordinator as soon as they become aware of the error. If the sender is unavailable or cannot recall the email for any reason, the Data Protection co-ordinator will ask the IT Lead to recall it.

In any cases where the recall is unsuccessful, the Data Protection co-ordinator will 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 Protection co-ordinator will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The Data Protection co-ordinator will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Photographs and Video

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 for photographs and videos to be taken of their child for communication, marketing and

promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Written consent will include a signature for each aspect of content. Uses 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 Twitter and Facebook 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.

Data Storage and Security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of records

Personal data that is no longer needed will be disposed of securely, in line with our retention policies. A copy of our retention policy is available to view in the school office. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. We will shred paper-based records and overwrite or delete electronic files.

Subject Access Requests

All staff, parents and other users are entitled to:

- Know what information the Academy holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the Academy is doing to comply with its obligations under the 1998 Act.

To address the first point, the Academy will, upon request, provide all staff and parents (and students when requested) and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Academy holds and processes about them, and the reasons for which they are processed.
All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.

The Academy will make a **maximum** charge of £10 (**Please refer to appendix B**) on each occasion that access is requested, although the Academy has discretion to waive this **under certain circumstances (e.g. if a parent requests information about their child regarding their education)**. The Academy will require that proof of ID is shown upon request.

The Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, although good practice recommends 15 working days, as required by the 1998 Act.

Training

Data protection will form part of continuing professional development for all staff and governors, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring

This policy will be reviewed every two years and shared with the full governing board.

Procedures agreed
January 2019

Appendix 1.

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection co-ordinator
- The breach should be reported using the GDPRIS system
- The Data Protection co-ordinator 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
- The Data Protection co-ordinator will alert the headteacher and the chair of governors

- The Data Protection co-ordinator will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The Data Protection co-ordinator will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Data Protection co-ordinator in conjunction with the Headteacher will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The Data Protection co-ordinator will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the GDPRIS database.
- Where the ICO must be notified, the Data Protection co-ordinator will do this via the 'report a breach' page of the ICO website within 72 hours. 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 Data Protection co-ordinator will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Data Protection co-ordinator expects to have further information. The DPO will submit the remaining information as soon as possible
- The Data Protection co-ordinator will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the Data Protection co-ordinator
    - 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 Data Protection co-ordinator will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Data Protection co-ordinator 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 the GDPRIS software
- The Data Protection co-ordinator and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Appendix 2 - Definitions

Personal data
Any information relating to an identified, or identifiable, individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data
Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing
Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject
The identified or identifiable individual whose personal data is held or processed.

Data controller
A person or organisation that determines the purposes and the means of processing of personal data.

Data processor
A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.