The Regis Academy

Version 1.0

Data Protection Policy

Date	**September 2020**
Date of Review	**August 2022**
Approved By	**A Pincher**

Aims

The Regis Academy holds a variety of personal information about staff, pupils and their parents / carers. We are aware of our data protection responsibilities for individuals that are the subject of data collection and retention; we will ensure that all data is treated fairly and lawfully.

We will ensure:

- that personal data is kept secure and confidential.

- to ensure employee's understand the importance of information rights as well as their own responsibilities for delivering them

Staff are required to report instances of non-compliance of data protection as outlined within this document. Failure to comply with this policy will be addressed without delay and may ultimately result in disciplinary action. Data protection and freedom of information The Data Protection Act (DPA) exists to protect people's right to privacy, whereas the Freedom of Information Act (FOIA) removes unnecessary secrecy. These two aims are not necessarily incompatible but there can be a tension between them and applying them sometimes requires careful consideration. Personal information requested by third parties is exempt from release under the FOIA where this release would breach the DPA. If a request is made for information that includes someone else's personal data, we will carefully balance the case for transparency and openness under the FOIA against the data subject's right to privacy under the DPA to decide whether the information can be released without breaching the data protection principles. The information may be issued by redacting / blanking out the relevant personal information. In some instances, we may consult with a third party if their interests could be affected by release of the information requested.

Complaints

All complaints are dealt with through the Complaints policy which is available on request at The Regis Academy or by calling 0121-565-4012.

If the response is not satisfactory after exhausting the complaints process, the complainant should contact the Information Commissioners Office (ICO).

Monitoring and Review

This policy will be reviewed every two years or in the following circumstances:

- Changes in legislation and/or government guidance

- As a result of any other significant change or event

- In the event that the policy is determined not to be effective any concerns should be raised with the Data Protection Officer on 0121-565-4012 in the first instance for them to determine whether a review of the policy is required in advance of the planned review date.

Processing Personal Data

The Regis Academy is registered with the ICO which complies with the DPA. We will only process personal data where there are legitimate grounds for collecting and using the

personal data. Data will not be used in ways that have unjustified or adverse effects on the individuals that the data concerns. Information will be:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Kept for no longer than is absolutely necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the UK without adequate protection

Data Gathering

All personal data relating to individuals gathered by The Regis Academy, whether held on computer, in paper files, are covered by the DPA. To process this data fairly, we will provide the data subject details about the data's intended use and inform them if the data may be used for other purposes or disclosed to another party. Individuals will be informed of this unless the collection and use of the data is:

- Something that a reasonable person is likely to anticipate and would agree to if asked.
- Is necessary to carry out the function the individual requested.
- Will have no unforeseen consequences for the individual concerned.

Information will be collected in a fair and open manner we will tell individuals how the information will be used and who will be allowed to see it. Privacy notices will be issued explaining the purpose of the data collection wherever necessary.

Data Checking

Reasonable steps will be taken to ensure the accuracy of personal data. In order to do this we will:

- Issue regular reminders to ensure that personal data held is up-to-date and accurate.
- Rectify any errors discovered and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.
- Make sure that the data provided is done so by the person it concerns (or someone acting on their behalf) and that any challenges to the accuracy of the information are carefully considered.

Data Retention

All personal data will be stored in a secure and safe manner in particular:

- Manual data will be stored where it not accessible to anyone without a legitimate reason to access it

- Particular attention will be paid to the need for security of sensitive personal data

Electronic Data

All computers will have adequate protection software, such as anti-virus, etc, which will be kept up to date. All unused or older versions of such software will be removed from the devices.

The use of mobile devices such as laptops may require additional protection; this will be proportionate to the level of risk associated with a particular device. Due to their portable nature, the chances of them being lost or stolen is increased therefore the personal data stored on such devices will be limited or removed.

All electronic data will be backed up on a regular basis and the backup will be kept securely and access will be restricted to essential staff members.

All staff members have been issued with an email address and access to secure sites. Security for these is of high importance and staff will be required to set strong passwords and renew passwords on a regular basis. Sending data from a personal email account should be avoided however there are certain situations where this may be acceptable with prior approval. This will be done on a limited basis.

Using Data

Personal data will not be used in any newsletters, websites or other media without the consent of the data subject. We may incorporate consent into the data gathering sheets, to avoid the need for frequent or similar requests for consent being made.

Sharing Data

Before sharing any personal data, we will consider all the legal implications of doing so. We will always inform individuals of our intention to share data (if this has not previously been communicated and will gain consent where it is required). Sharing without the individual's knowledge There may be instances where information is released to external bodies under one of the exemptions listed in the DPA. In particular this covers disclosing information for the prevention or detection of crime.

Archiving and Deleting Data

Personal data shall not be kept for longer than is necessary for the purpose it is collected. Data will be updated or archived if it goes out of date. If the data is no longer needed then it will be securely destroyed or deleted in line with retention policy. All paper waste will be shredded and electronic copies will be permanently removed from computers / hard drives.

Data will only be archived instead of deleted if the information still needs to be retained. If data is deleted from a live system then we will ensure that any form of back up or copy will also be deleted. All personal information is removed prior to the disposal or old computers. We will regularly review the data we hold and the length of time data is retained in accordance with regulatory and professional guidelines and our data and retention schedule.

We will conduct a regular audit, involving checking through records to make sure data is not retained for too long and to ensure that data is not being deleted prematurely.

Dealing with a Breach of the DPA

In the event of a data security breach Anna Pincher, Head of Centre must be informed immediately, who will then contact the Data Protection Officer at The Albion Foundation, Shin Aujla . If we become aware of a data breach we will:

- Investigate and contain the situation to limit the damage
- Assess the risks associated with the breach
- Identify potential adverse consequences for individuals
- Inform the appropriate people and organisations (ICO/police) that the breach has occurred
- Accurately record the details of the breach and the actions taken

Following a breach of personal data we will evaluate the cause of the breach and the action taken to prevent similar breaches occurring in the future.

CCTV

External or Internal CCTV is not in operation at the School, in the event of any changes the Data Protection Policy will be updated.

Subject Access Requests

The DPA gives individuals the right to find out what information the school stores about them. This is known as a Subject Access Request (SAR). If a data subject would like a copy of the information that is held about them then they must put this request in writing. The request can be sent by post or email. Informal requests (oral) will be dealt with wherever possible. As the data controller, The Regis Academy is responsible for compliance with the DPA and an individual's right to make a SAR. If a request is made that relates to data that is held centrally then The Regis Academy will respond directly to this.

We will make reasonable adjustments for individuals with disabilities who choose to make a SAR. This will be done in accordance with the Equality Act 2010 and the school's Equality Policy. We will make reasonable and proportionate efforts to find and retrieve the requested data in order to respond effectively to all SAR's. Information will be provided to the data subject in a permanent form unless the individual agrees otherwise, or doing so would be impossible or involve disproportionate effort.

Repeated, identical or similar SAR's made by the same person will not be responded to unless a reasonable interval has elapsed between the first request and any subsequent ones – if this occurs, we will inform the individual why the information has not been provided again.

Requests for Information about Pupils

We understand that personal data about a pupil belongs to the child and not their parent or carer. If a SAR is made on behalf of a pupil, then we will first consider whether the child understands their rights. If we are confident that they do then we will send the response of the SAR directly to the pupil the request is about. If we do not believe that the child understands their rights in regards to a SAR then we will also take into account the following factors before releasing the information to the child or person with parental responsibility:

- The pupil's level of maturity and their ability to make decisions like this
- The nature of the personal data
- Any court orders relating to parental access or responsibility that may apply
- Any duty of confidence owed to the child or young person
- Any consequences of allowing those with parental responsibility access to the information or any detriment to the pupil if the information is not disclosed
- Any views the pupil has on whether the information about them should be provided

When Information can be Withheld

There is a legal requirement to provide a data subject with a copy of the information that is held about them if it is requested. However, there are some instances where information can be withheld. The DPA provides a number of exemptions. The decision about whether to rely upon an exemption and withhold data is determined by The Regis Academy may be in relation to all of the information requested or just part of it.

If information is withheld in reliance on an exemption, we will respond promptly explaining, to the extent we can do so, the fact that information has been withheld and the reasons why. If only part of the information is withheld, then as much information as possible will be disclosed. Examples of information which the school may consider be appropriate to withhold include:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

If providing the information to an individual will disclose information about another person then we will only disclose this if we have received consent from the third party or it is considered reasonable in all the circumstances to comply with the request without consent. Information may be redacted that can identify another individual and where providing images from the CCTV system, images of third parties on the footage may be obscured or blurred.

Charges for SAR's A charge may apply for making a SAR. We will inform an individual of any charge we choose to apply without delay upon the receipt of the SAR. The following charges may apply: £10 for the majority of SAR's or up to £50 (dependent on the number of pages as detailed by the ICO) where a SAR is made for information containing, in whole or in part, a pupil's educational record

Time Limits

The time limit for responding to most SAR's is 40 calendar days. If the request is for a pupil's educational file then the time limit is 15 days. The time limit begins once the request has been received providing that:

- Any fee applicable is paid. There are no doubts as to the identity of the data subject
- The information requested is able to be located and identified from the SAR

If the request is made by a third party on someone else's behalf then they may need to provide evidence that they are entitled to do this, such as a power of attorney or letter of authority from the data subject. We will only request evidence or additional information if this is appropriate and considered necessary to ascertaining an individual's identity or to help us locate or identify the information.