Ormiston Sandwell Community Academy

Data Protection Policy

Date adopted: 15/1/18 Next review date: 15/1/20

Policy Version Control

Policy prepared by	OAT
Responsible committee	policies
Date approved by committee	4/11/15

Contents

1. Policy statement and principles

1.1 Policy aims and principles

Through day to day activities, Ormiston Sandwell Community Academy and OAT academies hold a variety of personal information about staff, students and their parents / guardians. In some instances information may be held about staff and students' family members, such as, next of kin. We are aware of our data protection responsibilities for individuals that are the subject of data collection and retention by OSCA or an OAT academy and we will ensure that all data is treated fairly and lawfully.

The principles behind this policy are:

- To ensure that personal data is kept secure and confidential – preventing information passing into the wrong hands and reducing the risks of fraud attacks
- To ensure employee's understand the importance of information rights as well as their own responsibilities for delivering them
- To save time, effort and money by having effective procedures in place

All employees are required to report instances of non-compliance of data protection principles detailed in this policy. All staff will have access to this policy and will be aware of who to contact with regards any of the procedures detailed.

This policy is consistent with all other policies adopted by OSCA and is written in line with current legislation and guidance. Failure to comply with this policy will be addressed without delay and may ultimately result in disciplinary action.

1.2 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.

1.3 Complaints

All complaints are dealt with under the **OSCA Complaints Policy**.

Complaints should be made in writing and will follow the OSCA complaint procedures and set timescales. The

handling of complaints may be delegated to an appropriate person.

The outcome of the complaint will be communicated in writing.

If the response is not satisfactory after exhausting the complaints process, the complainant should contact the Information Commissioners Office (ICO). The ICO can make a decision to investigate a claim against the academy and take action against anyone who has misused personal data.

The contact details for the ICO are:

Telephone: 0303 123 1113
Website: http://www.ico.org.uk/complaints

1.4 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

If there are urgent concerns these should be raised to the Data Protection Officer in the first instance for them to determine whether a review of the policy is required in advance of the planned review date.

2. Processing personal data

The DPA requires every organisation who is processing personal information to register with the ICO as a data controller. The registered data controller is OAT for all OAT academies.

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. We recognise that certain types of data are more sensitive by nature than others and a Privacy Impact Assessment (PIA) will be conducted to determine any risks associated with processing any data. 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

2.1 Data gathering

All personal data relating to individuals gathered by OAT or an OAT academy, whether held on computer, in paper files or other electronic media (CCTV), 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.

2.2 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

2.3 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, anti-malware or anti-spyware, 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 potable nature, the chances of them being lost or stolen is increased therefore the personal data stored on such devices will be limited or removed.

Lost or stolen devices must be reported to *OSCA* within 24 hours.

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. If there is the need to send group emails then the academy will avoid including others email addresses by using blind carbon copy (BCC) not carbon copy (CC).

2.4 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.

Publication of exam results

The DPA does not stop the publishing of examination results. Publication can be done in a variety of ways, including posting lists of results on publicly accessible noticeboards, or providing examination results to the media.

We will act fairly in our decision to publish exam results and inform those involved whether results will be made public and how this will be done. This will be done as early as possible, at the start of the academic year and during each examination term.

Any concerns raised will be taken seriously and we will consider any objections before deciding to publish results and will provide the reason if a person's objection is rejected.

2.5 Sharing data

Before sharing any personal data, we will consider all the legal implications of doing so and undertake a PIA to consider the potential benefits and risks of sharing data. 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).

When sharing data, we will put in place a data sharing agreement and ensure that the information is passed on in a secure way. Only the minimum information will be shared for the purpose of the agreement to meet the objectives, in all instances where the objectives can be met by anonymising data this will be done. A record will be kept of all data sharing agreements and will regularly review the agreements to ensure that data is not being shared unnecessarily.

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.

2.6 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 *OAT's /OSCA's* retention and deletion schedule. 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.

2.7 Dealing with a breach of the DPA

In the event of a data security breach *Sue Bowron (Financial Director/Data Protection Officer)* must be informed immediately. 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 that the breach has occurred
- Accurately record the details of the breach and the actions taken
- Where appropriate, inform the ICO and / or other third parties (police, insurers, professional bodies)

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.

3. CCTV

CCTV is used in OAT offices and on academy premises to promote the safety and welfare of all individuals accessing the facilities. Images of people are covered by the DPA, this includes the information that can be derived from images. The CCTV system will only capture images of individuals and will not be used for audio recording.

The use of CCTV will be reviewed annually to ensure that it is effective.

All reasonable steps will be taken to ensure that individuals are aware that CCTV is in operation in specific areas.

The system used will have the necessary technical specification to ensure that images are of the appropriate quality and are not obstructed in any way. Cameras have been sited so that they provide clear images and so that they avoid capturing the images of individuals that is does not intend to capture. Regular checks will be carried out to ensure that the system is working properly and produces high quality images, this will include a check that the date and time stamp recorded on the images is accurate.

Images from the CCTV system are securely stored and only a limited number of authorised personnel may have access to them. The viewing of live images on monitors will be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.

The images will, in most instances, not be provided to any third parties with the exception of law enforcement bodies.

Requests for copies of an individual's own images will be dealt with as a Subject Access Request as detailed in section 4 of this policy. We have discretion to refuse any request for information unless there is an overriding legal obligation to do so.

If images are disclosed then the method of disclosing them will be secure, ensuring that they are only seen by the intended recipient.

Once there is no reason to retain the recorded images, they will be deleted. The recorded images will only be retained long enough for:

- Any incident to come to light
- And the incident to be investigated

If at any point the use of CCTV processing requires working with another organisation, the academy will have a written contract with the processor which specifies exactly how the information is to be used and gives security guarantees.

3.1 Monitoring staff

The use of CCTV is not intended to be used to monitor staff however they may be used if an incident arises that involves a member of staff or if something is seen on the footage that we cannot be expected to ignore, such as criminal activity, gross misconduct, or behaviour which puts others at risk.

If images are used in disciplinary proceedings, the footage will be retained so that the member of staff can see it and respond.

4. Subject access requests

The DPA gives individuals the right to find out what information OAT and / or an OAT academy 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, fax and email or via our social media sites however the preferred means of contact for such a request is either by post or email the data request to OAT or directly to Ormiston Sandwell Community Academy. Informal requests (oral) will be dealt with wherever possible.

As the data controller, OAT 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 (by OAT) then OAT will respond directly to this. If the request relates to data that an OAT academy holds then the responsibility for responding to a SAR will be delegated to the academy involved.

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 OAT'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.

4.1 Requests for information about children

We understand that personal data about a child belongs to the child and not their parent or guardian. If a SAR is made on behalf of a child 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 child 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 child'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 child if the information is not disclosed
- Any views the child has on whether the information about them should be provided

4.2 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 OAT and the academy and 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 academy may consider be appropriate to withhold include:

- Information that might cause serious harm to the physical or mental health of the student 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.

4.3 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 (exempt from VAT) may apply:

- £10 for the majority of SAR's
- £10 per disk for copies of CCTV footage
- 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 student's educational record

4.4 Time limits

The time limit for responding to most SAR's is 40 calendar days. If the request is for a student's educational file then the time limit is 15 academy 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 we need to request payment and / or additional information the time limit will not begin until the data subject has provided payment and / or the information required.

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.