# DATA PROTECTION POLICY

**The OHC&AT Board of Directors has agreed this Policy and as such, it applies across the organisation – 29th June 2018.**

Jay Mercer
Chair of OHCAT Board

Darren Coghlan
Chair of OHC Board

# Data Protection Policy

## INTRODUCTION

Orchard Hill College and Academy Trust (OHC&AT) is committed to providing outstanding educational opportunities for all our pupils and students. This policy is intended to ensure that 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 expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. The policy complies with the Academy Trust's Master Funding Agreement and Articles of Association as well as the College's Articles of Association.

It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities and will at all times abide by the following principles: ask permission, respect the privacy of the subject, and value and protect their data.

OHC&AT will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes for which it was collected.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

OHC&AT comprises two separate legal entities, Orchard Hill College (OHC) and Orchard Hill College Academy Trust (OHCAT) working together to deliver educational excellence. Any and all references to OHC&AT should be assumed to apply to both OHC and OHCAT.

## STATEMENT OF INTENT

OHC&AT collects and uses personal information about pupils/students, staff, parents/carers and other individuals who come into contact with the organisation. This information is gathered in order to enable OHC&AT to provide education and associated functions. In addition, there may be a legal requirement to collect and use information to ensure that OHC&AT complies with its statutory obligations.

Schools and colleges have a duty to be registered as Data Controllers with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on the ICO website. Schools and colleges also have a duty to issue a Fair Processing Notice to all pupils/students/parents/carers: this summarises the information held on pupils/students, why it is held and the other parties to whom it may be passed on.

OHC&AT's Data Protection Registration numbers can be found at the end of this policy.

OHC&AT will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the OHC&AT community to take care, when handling, using or transferring personal data, to ensure that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or organisations, can bring the organisation into disrepute and may result in disciplinary action, criminal prosecution and fines imposed by the ICO on OHC&AT and the individuals involved.

Particularly, all transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

## DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that OHC&AT and its academies and College centres must comply with. The principles say that personal data must be:

- Processed with the clear consent of the individual
- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how OHC&AT aims to comply with these principles.

OHC&AT is committed to maintaining these principles at all times. Therefore the organisation will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed, it is done so appropriately and securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information (Subject Access Requests)
- Ensure that OHC&AT staff are aware of and understand our policies and procedures

Everyone in the organisation has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors and Directors are required to comply fully with this policy in the event that they have access to personal data when engaged in their respective roles.

## PERSONAL DATA

Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held.

OHC&AT and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the OHC&AT community, including pupils/students, members of staff and parents/carers, e.g. names, addresses, contact details, legal guardianship details, health records, disciplinary records etc.
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references.
- Professional records e.g. employment history, taxation and National Insurance records, appraisal records and references.
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Requests from Police or other official bodies for personal information should be made via the form in Appendix 2.

## RESPONSIBILITIES

**It is incumbent upon all staff, governors, volunteers and other members of the OHC&AT community to ensure that personal data is handled in a safe and secure manner.**

**OHC&AT Directors will:**

- Review and approve this and any related policies and procedures at least every three years or as required

**The OHC&AT Director of Business Services will:**

- Act as the Data Protection Officer (DPO) for the organisation and assume all related responsibilities including:
    - Overseeing the implementation of this policy, monitoring compliance with data protection legislation and developing related policies and procedures where applicable;
    - Regularly reporting to the Executive Senior Leadership Team (ESLT) on data protection compliance matters;
    - Reporting annually to OHC&AT Directors on data protection compliance matters, including any recommendations and advice regarding data protection issues.

OHC&AT's appointed Caldicott Guardian is the **Director of Safeguarding & Learning Support Services**. The role of the Caldicott Guardian exists to safeguard the privacy interests of patients, in accordance with the Caldicott Report requirements for the protection of patient identifiable information. It is important that every interaction with the NHS, other providers and patients is conducted in an ethical manner with due thought to the potential implications.

The Caldicott Principles are:

- Justify the purpose(s) of using confidential data
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need-to-know basis
- Everyone must understand his/her responsibilities
- Understand and comply with the law

The role of the Caldicott Guardian is to:

- develop local protocols governing the disclosure of patient identifiable information to other organisations
- restrict access to patient information within each organisation by enforcing strict need to know principles
- regularly review and justify the uses of patient information
- improve organisational performance across a range of related areas: database design, staff induction, training, compliance with guidance etc.

**Governors and Directors will:**

- Ensure that they comply with all necessary data protection requirements in the pursuance of their duties
- Offer appropriate support and challenge to their Academy/College leadership teams regarding data protection issues

**Principals will:**

- Act as the representative of the Data Protection Officer on a day to day basis within their respective provisions.

**All staff will:**

- Collect, store and process any personal data in accordance with this policy
- Inform OHC&AT of any changes to their personal data e.g. change of address
- Contact the DPO for further advice and guidance regarding data protection and processing issues, including (but not limited to):
    - if they require any further guidance on adhering to this policy
    - if they have any concerns about the safe processing of personal data within the organisation
    - in order to ascertain the legal basis to use personal data in a particular way
    - if there has been a data breach

## COLLECTING PERSONAL DATA

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 OHC&AT can fulfil a contract with the individual, or the individual has asked OHC&AT to take specific steps before entering into a contract
- The data needs to be processed so that OHC&AT 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 OHC&AT, 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 OHC&AT 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 pupil/student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

OHC&AT provisions which offer online services to pupils/students e.g. classroom apps, and which intend to rely on consent as a basis for processing, will get parental consent where the pupil/student is under 13 or where they do not have capacity to consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with OHC&AT's Information and Record Retention Policy.

## SHARING PERSONAL DATA

OHC&AT will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil/student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our pupils/students and staff – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and Local Authorities to help them to respond to an emergency situation that affects any of our pupils/students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF THE INDIVIDUAL

Individuals have a right to make a Subject Access Request (SAR) to gain access to personal information that OHC&AT holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned

- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject Access Requests should be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a SAR they must immediately forward it to the DPO.

Please see Appendix 1 for full details of the Subject Access Request procedure.

**Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Additionally, special educational needs and disabilities may impact upon a child or young person's ability to give consent. OHC&AT will always apply the principles of the Mental Capacity Act in determining whether any individual pupil or student has capacity to consent to a specific occurrence such as a SAR.

**Responding to Subject Access Requests**

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil/student or another individual
- Would reveal that the pupil/student is at risk of abuse, where the disclosure of that information would not be in the pupil/student's best interests
- Is contained in adoption or parental order records

- Is given to a court in proceedings concerning the pupil/student

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and inform them of their right to complain to the ICO.

**Other data protection rights of the individual**

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

**BIOMETRIC RECOGNITION SYSTEMS**

Where we use pupils'/students' biometric data as part of an automated biometric recognition system (for example, pupils/students using finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy/College will get written consent from the pupil/student and/or at least one parent or carer before any biometric data is taken and first processed.

Parents/carers and pupils/students have the right to choose not to use biometric systems. We will provide alternative means of accessing the relevant services for those pupils/students.

Parents/carers and pupils/students can object to participation in biometric recognition systems, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil/student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil/student's parent or carer.

Where staff members or other adults use biometric systems within OHC&AT provision, we will obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and OHC&AT will delete any relevant data already captured.

## CCTV

OHC&AT provisions may use CCTV in various locations around their sites in order to ensure the safety of pupils/students, staff and the site itself. OHC&AT adheres to the ICO's code of practice for the use of CCTV. All CCTV usage is clearly signposted and individuals are made aware that they are being recorded.

## PHOTOGRAPHS AND VIDEOS

As part of our educational activities, OHC&AT staff may take photographs and record images of individuals within our provisions.

We will obtain written consent from parents/carers and/or pupils/students, depending on their age and capacity to consent, for photographs and videos of pupils/students to be taken for communication, marketing and promotional materials. We will clearly explain to both the parent/carer and the pupil/student how the photograph and/or video will be used.

Uses may include:

- Within Academies/College centres on notice boards and in Academy/College magazines, brochures, newsletters, etc.
- Outside of OHC&AT provisions by external agencies such as the school photographer, newspapers, campaigns etc.
- Online on OHC&AT websites 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 pupil/student, to ensure they cannot be identified.

Once pupils/students have left OHC&AT provisions, any photos/videos of them will be removed from OHC&AT use as far as is possible e.g. deleted from websites, presentations and central files.

## DATA PROTECTION BY DESIGN AND DEFAULT

OHC&AT has put measures in place to integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Ensuring that staff receive regular training on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and ensure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the organisation and the DPO as well as all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## DATA SECURITY AND STORAGE OF RECORDS

### Physical security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed access to personal files. Information will be locked away securely when not in use. Visitors to OHC&AT settings are required to sign in and out, to wear identification badges whilst on OHC&AT property and are accompanied by OHC&AT staff where appropriate.

OHC&AT operates a Clean Desk Policy across all its sites:

- At known extended periods away from their desks, such as a lunch break, staff should place sensitive working papers in locked drawers.

- At the end of the working day staff should tidy their desks and store all papers and other work-related materials/storage devices in a suitable place e.g. locking desk pedestal or filing cabinet.
- Personal or confidential business information must be protected using security features provided, for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Staff should take care not to leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

**Data storage and access**

OHC&AT will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Users will use strong passwords which must be changed regularly. Passwords must be changed immediately if staff suspect their security has been breached. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods).

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. In the event that personal data must be taken outside of OHC&AT locations e.g. working from home or travelling to meetings, staff must take extra precautions to ensure that the data is securely stored at all times.

Personal data can only be stored on OHC&AT equipment (this includes computers and portable storage media). User-owned equipment must not be used for the storage of personal data. In particular, staff **must not** take photographs of pupils or students on their personal devices.

When personal data is stored on any portable computer system, USB stick or other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device in line with OHC&AT policy once it has been transferred or its use is complete

OHC&AT has clear policies and procedures for the automatic backing up, accessing and restoring of all data held on OHC&AT systems (see Related Policies and Procedures).

Paper-based protected and restricted material must be held in lockable storage, regardless of location.

OHC&AT recognises the rights of the individual in connection with their personal data. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to:

- know if the data controller holds personal data about them;
- see a description of that data;
- know the purpose for which the data is processed;
- know the sources of that data;
- know to whom the data may be disclosed;
- receive a copy of all the personal data that is held about them.

Under certain circumstances the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data. Where a request includes data about another person, information may be redacted to protect that person's data.

**Secure transfer of data and access outside of OHC&AT settings**

OHC&AT recognises that personal data may be accessed by users outside of OHC&AT settings, or transferred to local authorities or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from OHC&AT premises without permission and unless the media is encrypted, password protected and transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when outside OHC&AT premises.
- When restricted or protected personal data is required by an authorised user outside of the organisation's premises (e.g. by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- When restricted or protected personal data is required in **paper-based** format by an authorised user outside of the organisation's premises (e.g. by a member of staff to work from their home), they must take extra precautions to securely store the information and minimise the risk of physical loss and/or degradation.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from OHC&AT premises if the storage media, portable or mobile device is encrypted and transported securely for storage in a secure location.

- Where files containing personal data need to be sent via email, the file must be password protected and the password conveyed separately to the recipient.
- All portable and mobile devices and storage media used to store and transmit personal information must be protected using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

**Disposal of data**

OHC&AT will comply with the requirements for the safe destruction of personal data when it is no longer required.

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of each Principal to ensure that obsolete data is properly erased within their provision.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance; other media must be shredded, incinerated or otherwise disintegrated for data.

**Audit logging/reporting/incident handling**

In the event of an information risk incident, the complaints procedure in the OHC&AT Complaints Policy should be followed. This procedure allows for reporting, managing and recovering from information risk incidents by establishing:

- a ‘responsible person’ for each incident;
- a communications plan, including escalation procedures;

and resulting in:

- a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported either to the OHC&AT CEO/Principal or to the DPO who will then contact the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

**Websites and social media**

OHC&AT will ensure that no personal information, including images, will be published on OHC&AT websites or social media e.g. official Twitter account, without permission from the individual/s concerned. Pupil/student and staff access to websites and social media groups is monitored by OHC&AT on a regular basis.

## PERSONAL DATA BREACHES

OHC&AT will make all reasonable endeavours 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 3.

- When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an educational context may include, but are not limited to:
    - A non-anonymised dataset being published on an Academy website which shows the exam results of pupils eligible for the pupil premium
    - Safeguarding information being made available to an unauthorised person
    - The theft of a College laptop containing non-encrypted personal data about students

## TRAINING

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or OHC&AT processes make it necessary.

## POLICY REVIEW DETAILS

| | |
|---|---|
| *Version:* | 1.4 |
| *Reviewer:* | Janet Sherborne |
| *Approval body:* | Family Board |
| *Date this version approved:* | 29th June 2018 |
| *Due for review:* | Summer 2019 |

## RELATED POLICIES AND PROCEDURES

Child Protection Adult Protection & Safeguarding Policy
Complaints Policy
E-Safety Policy
Information and Records Retention Policy
IT Acceptable Use Policy and Appendices
Mental Capacity and Consent Policy
Photo Permission Policy
Staff Code of Conduct

## FURTHER INFORMATION

Information Commissioner's Office
www.ico.gov.uk
0303 123 1113 or 01625 545745

OHC&AT Data Protection Registration numbers:

- Orchard Hill College: ZA217813
- Orchard Hill College Academy Trust: ZA048879

## APPENDIX 1: SUBJECT ACCESS REQUESTS

### Rights of access to information

There are two distinct rights of access to information held by schools and colleges about pupils and students:

1. Under the General Data Protection Regulation (GDPR) 2018, any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records are defined within the Education Pupil Information (England) Regulations 2005.

These procedures relate to subject access requests made under the GDPR.

### Actioning a SAR

1. The GDPR does not specify that requests must be made in writing, and therefore OHC&AT staff will be alert to any subject access request made verbally, in writing or via other channels such as social media. All requests must be referred to the DPO.
2. If the initial request does not clearly identify the information required, further enquiries will be made.

3. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the pupil or student where relevant. Evidence of identity can be established by requesting production of:
    - passport
    - driving licence
    - utility bills with the current address
    - birth or marriage certificate
    - P45/P60
    - credit card or mortgage statement

    This list is not exhaustive.

4. Any individual has the right of access to information held about them. However, the nature of the request and the capacity of the subject to give consent must be taken into account. The DPO should discuss the request with the pupil/student and take their views into account when making a decision. A pupil/student with capacity to consent can refuse to consent to the request for their records. Where the pupil/student is not deemed capable of consent, an individual with parental responsibility or guardian shall make the decision on behalf of the pupil/student.

5. OHC&AT will not make a charge for the provision of information, except in circumstances where the request is manifestly unfounded or excessive, in which case a reasonable fee may be charged in order to comply with the request. This is in accordance with ICO guidelines.

6. The response time for subject access requests, once officially received, is one month irrespective of any holiday or non-working periods.

7. The response time for student information requests, once officially received, is 20 calendar days irrespective of any holiday or non-working periods. However, the 20 days will not commence until after receipt of identification and clarification of information sought, if required.

8. A Freedom of Information Request can be initiated by any person. The information disclosed through an FOI request will usually become public information, available to anyone. The response therefore cannot include personal or sensitive information, as these are exempt from FOI requests. This may be subject to a fee, to be determined on a case by case basis by the relevant OHC&AT setting.

   The response time for Freedom of Information requests, once officially received, is 20 days irrespective of any holiday or non-working periods. However, the 20 days will not commence until after receipt of fees and clarification of information sought, if required.

9. The GDPR allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

10. Third party information is that which has been provided by another, such as the police, local authority, health care professional or another educational provider. Before disclosing third party information consent should normally be obtained. There is a still a need to adhere to the one month statutory timescale.

11. Any information which may cause serious harm to the physical or mental health of emotional condition of a pupil/student or another should not be disclosed. Nor should information that would reveal that the pupil/student is at risk of abuse, or information relating to court proceedings.

12. If there are concerns over the disclosure of information then additional advice should be sought.

13. Where redaction (information blacked out/removed) has taken place, a full copy of the information provided should be retained in case of complaint in order to establish what was redacted and why.

14. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained.

15. Information can be provided at the relevant OHC&AT setting with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, registered/recorded mail must be employed.

## APPENDIX 2: POLICE REQUEST FORM FOR PERSONAL DATA

TO: _____

Please complete in full and fax to 020 8254 9800
For the attention of the Marketing Manager, Orchard Hill College and Academy Trust

---

**Data Protection Act 1984 – Section 28 (3)**

I am making enquiries which are concerned with:

a. The prevention or detection of crime, or*

b. The apprehension or prosecution of offenders*

c. The urgent prevention of injury or damage to health*

*Delete as appropriate (*)*

| Information required: |
| --- |
| |

Name and rank: _____

Signed: _____ Date: _____

Address and telephone number of station:

_____

_____

_____

_____

_____

## APPENDIX 3: PERSONAL DATA BREACH PROCEDURE

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 DPO. 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

The DPO will alert the Principal and the Chair of Governors of the relevant OHC&AT provision.

The DPO 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 DPO will assess the potential consequences, based on how serious they are and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO 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 DPO 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. Records of decisions will be stored in an appropriate file on the OHC&AT Management Drive.

Where the ICO must be notified, the DPO 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 DPO 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO 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 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 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 in an appropriate file on the OHC&AT Management Drive.

The DPO 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.

**Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, 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 DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO 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