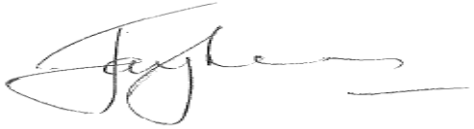
DATA PROTECTION POLICY

The OHC&AT Board of Directors has agreed this Policy and as such, it applies across the organisation – 15th December 2017.

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 information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. 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 by adhering to these guidelines.

OHC&AT will hold the minimum personal data necessary to enable it to perform its function and it 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.

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 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 Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

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

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

OHC&AT's Senior Information Risk Officer (SIRO) is the Executive Director, OHC&AT Services. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for OHC&AT's Data Protection Policy and risk assessment;
- appoint the Information Asset Owners (IAOs).

OHC&AT will identify Information Asset Owners (IAOs) for the various types of data being held e.g. student information, staff information, assessment data etc. The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose;

- how information has been amended or added to over time;
- who has access to protected data and why.

OHC&AT's appointed Caldicott Guardian is the Director of 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 are required to comply fully with this policy in the event that they have access to personal data when engaged in their governance role.

Information for parents/carers – Privacy Notice

In order to comply with the fair processing requirements of the DPA, OHC&AT will inform parents and carers of all pupils and students of the data it collects, processes and holds on pupils/students, the purposes for which the data is held and the third parties (e.g. LA, DfE) to whom it may be passed. This privacy notice will be passed to parents/carers through the website of the relevant OHC&AT setting.

Training and awareness

Staff will receive data handling awareness/data protection training and will be made aware of their responsibilities as described in this policy, through:

- Induction training for new staff
- Staff handbook/induction handbook
- Staff meetings/briefings and Inset days
- Day to day support and guidance from Information Asset Owners

DATA PROTECTION

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 that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. 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 Head/Principal to ensure that obsolete data is properly erased.

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

It is good practice, as recommended in 'Data Handling Procedures in Government' (Cabinet Office, 2008), that the activities of data users in respect of electronically held personal data will be logged and these logs will be monitored by responsible individuals. The audit logs will be kept to provide evidence of accidental or deliberate data security breaches, including e.g. loss of protected data or breaches of an acceptable use policy.

In the event of an information risk incident, the complaints procedure in the OHC&AT Compliments and 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 Principal/CEO or to the Senior Information Risk Officer (SIRO) 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.

CCTV

Images of people are covered by the Data Protection Act, and so is information about people which is derived from images e.g. vehicle registration numbers. Where CCTV is used on OHC&AT premises, we will ensure that we tell people if it is in use.

Complaints

Complaints will be handled in accordance with OHC&AT's Compliments and Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

POLICY REVIEW DETAILS

Version:	1.3
Reviewer:	Janet Sherborne
Approval body:	Family Board
Date this version approved:	15th December 2017
Due for review:	Spring 2020

RELATED POLICIES AND PROCEDURES

Child Protection (Safeguarding) Policy
Photo Permission Policy

IT Acceptable Use Policy and Appendices
Compliments and Complaints Policy
E-Safety Policy
Mental Capacity and Consent Policy

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 Data Protection Act 1998 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 as defined within the Education Pupil Information (England) Regulations 2005.

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

Actioning a SAR

1. Requests for information must be made in writing, including email, and be addressed to the OHC&AT Executive Director (Services). If the initial request does not clearly identify the information required, further enquiries will be made.

2. 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.

3. 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 Senior Information Risk Officer (SIRO) 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.

4. OHC&AT may make a charge for the provision of information, dependent on the following:
    - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
    - Should the information requested be personal information that does not include any information contained within educational records, OHC&AT can charge up to £10 to provide it.

- If the information requested is only the educational record, viewing will be free but a charge not exceeding the cost of copying the information can be made by OHC&AT.

5. The response time for subject access requests, once officially received, is 40 calendar days irrespective of any holiday or non-working periods. However, the 40 days will not commence until after receipt of fees or clarification of information sought, if required.

6. 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.

7. 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.

8. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

9. 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 40 day statutory timescale.

10. 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.

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

12. 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.

13. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, it should be retyped.

14. 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:

_____

_____

_____

_____

_____