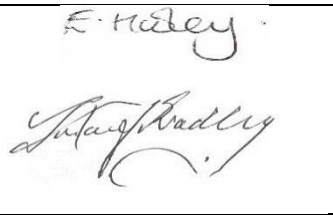
DATA PROTECTION POLICY

PERSON RESPONSIBLE FOR POLICY:	Mrs E Hooley
APPROVED:	17.5.18
SIGNED: **Headteacher** **Chair of Board of Trustees**	
TO BE REVIEWED:	May 2021
Data Protection Officer	Jessica Pembroke

DATA PROTECTION POLICY

1. Introduction

The Oaks Academy (the Academy) needs to process information about its employees, students and other individuals to allow it to monitor, for example, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Academy must comply with the Data Protection Principles.

The Academy and all staff or others who process or use any personal information must ensure that they follow these principles at all times. To achieve this, we will:

- Ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals. We will inform people what data we collect and why, through a Privacy Notice
- Ensure that personal information is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only process personal information for specific reasons, these include fulfilment of a contract (with a parent to provide childcare services or with an employee under their contract of employment)
- We will only share personal information where we have specific explicit consent or a legal basis to do so
- Ensure that where we ask for consent to use personal data we will ensure that we ask people to positively opt in, we use clear, plain language that is easy to understand, we specify why we want the data and what we're going to do with it, we tell individuals they can withdraw their consent, we ensure that individuals can refuse to consent without detriment and we avoid making consent a precondition of a service
- Ensure that all information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected
- Ensure that all information is kept accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay
- Implement appropriate record keeping standards and keep information in an identifiable form for no longer than is necessary for the purposes for which the personal data is obtained
- Ensure information is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and operational measures
- Demonstrate compliance with these requirements through appropriate documentation, training, spot checks and audits
- Comply with the rights for data subjects
- Ensure that every instance where we use a data processor (a third party with access to process personal data) we will have a written contract in place. Contracts will be provided by the Legal Advisor / Data Protection Officer
- Conduct a Data Privacy Impact Assessment (DPIA) where we are required to do so by law or best practice
- Report any data breaches promptly (using the form provided) and inform the ICO (Information Commissioner's Office) and data subjects where required

2. Status of the Policy

This Policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Academy from time to time. Any failures to follow the Policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the Policy has not been followed in respect of personal data about them, should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be raised as a formal grievance.

Compliance with data protection law is the responsibility of all members of the Academy. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Academy facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

3. Roles and Responsibilities

3.1. Senior Leadership Team

Overall accountability for data protection sits with the Senior Leadership Team (SLT).

The SLT will:

- Establish a data protection culture in the organisation
- Ensure the Academy has appointed an appropriate Data Protection Officer
- Ensure the Data Protection Officer operates independently and is not dismissed or penalised for performing their task (in relation only to their role as Data Protection Officer as defined in law)
- Ensure that adequate resources are devoted to meet the Academy's data protection obligations
- Commission reports from the Data Protection Officer and take action to remedy deficiencies identified by the report in a timely manner

3.2. Board of Trustees

The Trustees are responsible for holding the Senior Leadership Team to account to ensure compliance with the law.

The Data Protection Officer has a direct reporting line to the Trustees where they can raise any data protection risks or compliance issues.

3.3. Data Protection Officer

Operational responsibility for data protection sits with the Academy's Data Protection Officer.

The Data Protection Officer will:

- Inform and advise all members of staff on their data protection obligations
- Monitor compliance with data protection requirements

- Contribute to the development and maintenance of all data protection policies, procedures and processes in relation to the protection of personal data
- Advise and inform the Academy on any data protection impact assessment (DPIA), including monitoring performance of DPIAs
- Report and advise SLT on the allocation of their responsibilities to support ongoing compliance Data Protection law
- Provide data protection training and awareness to all members of staff
- Conduct audits of processes relating to personal data
- Be the point of contact for data subjects with regard to the processing of their personal data and respond to all data subject access request
- Advise senior management on the allocation of information security responsibilities
- Develop/advise on formal procedures for reporting incidents and investigations
- Contribute to the risk management, business continuity and disaster recovery planning process
- Advise on and monitor organisational record management and retention arrangements
- Ensure that records of the processing are kept and the Academy Notifies with the ICO
- Advise on the issuing of privacy notices to data subjects at the point of collection of their personal data
- Be the first point of contact for any enquiries from the Information Commissioners Office (and any other EU supervisory authorities)

3.4. Responsibilities of Staff

All staff will:

- Ensure any personal data which they hold is kept securely
- Ensure personal information is not disclosed either orally or in writing, accidentally or otherwise unlawfully to any unauthorised party
- Only access personal data that is applicable and required for them to undertake their role
- Complete and submit a data breach form at the first opportunity if and when any data breach occurs
- Undertake all required data protection training
- Maintain data protection awareness at all times reporting any data protection risks or concerns to their Line Manager or the Data Protection Officer
- Ensure that records are accurate, kept up to date kept securely and disposed of safely in accordance with the timescales set out in this policy
- Only send marketing information if they have consent from the data subjects and approval from the SLT and Data Protection Officer
- Not process Special Categories of data or Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer
- Ensure they have an appropriate contract in place (approved by the Data Protection Officer) with any third-party organisation that will have access to personal data
- Check that any information that they provide to the Academy in connection with their employment is accurate and up to date and inform the Academy of any changes to information which they have provided, e.g. change of address or name
- Comply with the security measures set out as follows:

Security Measures:

Physical Security:

- Staff must wear their ID badge at all times
- Staff must never allow others to use their swipe cards or pin numbers to gain entry
- Staff must not allow others to 'tailgate' e.g. follow a staff member through secure areas
- Staff must report to the school offcie if they encounter unescorted visitors or anyone not wearing appropriate visible identification, (i.e. an ID badge).
- Boards displaying person identifiable data should be sited in areas not accessible to the students or the public

Paper Record Security:

- All paper and files containing data subject details to be securely locked away when not in use a "clear desk policy"
- Data that is no longer required must be disposed of securely. The Academy uses a secure shredding company to dispose of data securely

Working remotely/offsite:

- Copies of physical records must only be taken off-site where absolutely necessary
- Only take the minimum necessary personal information off site
- Never take the master records off-site (only copies of the parts of the record necessary for the purpose)
- Ensure that staff members have a secure place to protect manual information when not at home
- Never leave personal information in an unsecure area in the home, i.e. in garages, sheds, boots of cars, near open doors or windows
- Never work on personal information in a public place where it could be seen by a third party
- Prevent access to information by other members of the household and by visitors. Staff members working from home should ensure they adopt a clear desk policy when leaving their work unattended

Transporting Paper Records:

- Keep information in a sealed container/bag
- Public transport should not be used for transporting personal information, if an exception to this rule is identified the information must be transported in a locked briefcase or similar
- Never leave information unattended in the car for an extended length of time
- Never leave information in the boot of a car overnight. Information must be taken inside a property and secured

When sending information by post:

- All external post should be delivered to the Post Room which must be locked when not staffed
- Post should not be left in unsupervised areas that are open to students or the general public
- Post containing personal or confidential information should be sent in sealed envelopes

IT Security:

- Screens of computers must always be locked when left unattended
- If electronic data is stored on removable media (like a CD or DVD), these must be encrypted and kept locked away securely when not in use
- Electronic data should only be stored on the Academy's designated drives and servers and should only be uploaded to an approved cloud computing services that the Academy has a contract with (e.g. do not use Dropbox, Google Drive etc.).

Sending information by email:

- Consider if email is the best communication method.
- Consider whether the e-mail going to just one person. If so, is it the correct person where similar names exist in the e-mail directory or address book
- Consider whether to use the 'reply all' function. If so, does every person on the list need to receive the reply and any attachment.
- Carefully check the recipients of all e-mails prior to sending regardless of content. Staff members should be extra vigilant where personal, sensitive personal or confidential information is included
- Delete emails which they have reached their retention period
- Only send email from another member of staff's email account or under an assumed name if they have the specific authority. This is generally reserved for personal assistants to Directors
- Manage email appropriately; clearing the deleted items folder and using appropriate archiving facilities
- Password protect the content of any email when sending sensitive/confidential/special categories of data

3.5. Parent Obligations

Parents must ensure that all personal data provided to the Academy is accurate and up to date. They must ensure that changes of address, etc., are notified to the school office.

4. Data Protection Principles

The data protection principles set out the Academy's main responsibilities.

Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In addition, the law requires that the Academy demonstrates compliance with these principles. This is known as the Accountability Principle.

The Academy's process for compliance with these principles is set out Appendix 1 – Data Protection Principles: Compliance.

5. Rights of Data Subjects

Data Protection law provides a set of rights for data subjects. These are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

These rights must be complied with within one month (this can be extended by two months where the request is complex). Where the timescale is extended the Academy must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Detailed guidance on compliance with these rights is set out at Appendix 2 – Data Subjects Rights.

6. Data Protection Impact Assessments (DPIA)

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help identify the most effective way to comply with data protection obligations. An effective DPIA will allow the Academy to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance.

The Data Protection Officer support employees undertaking a DPIA and will provide advice and will monitor the performance of the DPIA.

Where appropriate the Academy shall seek the views of data subjects or their representatives e.g. affected customers, members, partner organisations or employees as part of undertaking the DPIA. Where appropriate the Academy will also consult with the ICO.

7. International Transfers

Data Protection law imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individual's data is not undermined. Where staff are required to sending personal data to outside the European Union, to third countries or international organisations they must seek advice from the Data Protection Officer.

8. Breach Management

It is essential that all data protection incidents or near misses are handled appropriately. Where a data protection incident or potential incident has been identified staff should complete the form in Appendix 8 and forward this to the Data Protection Officer via dataprotect@ccsw.ac.uk who will follow the process set out at Appendix 8 to investigate the breach.

9. References

ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: 4 October 2017

http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), licensed under the Open Government Licence

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Appendix 1 – Key Definitions

Personal data	'personal data' means any information relating to an identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Special categories of personal data	'Special categories of personal data' are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Note: This was previously referred to as Sensitive Personal data
Processing	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Data Controller	'controller' any person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Processor	'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Data Protection law	Refers to the applicable laws of the land including once enforce the UK Data Protection Act 2018 and the EU General Data Protection Regulations

Appendix 2 - Data Protection Principles: Compliance

Principle 1 – Fair, Lawful and Transparent

Lawful Basis for Processing

The Academy must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing:

(a) Consent: the individual has given clear consent for the Academy to process their personal data for a specific purpose[1]
(b) Contract: the processing is necessary for a contract, or for specific steps before entering into a contract (e.g. the Academy's Contract of Employment with its Employees)
(c) Legal obligation: the processing is necessary for the Academy to comply with the law (not including contractual obligations)
(d) Vital interests: the processing is necessary to protect someone's life
(e) Public task: the processing is necessary for the Academy to perform a task in the public interest or its official functions, and the task or function has a clear basis in law
(f) Legitimate interests: the processing is necessary for the Academy's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply where we are acting as public authority processing data to perform our official tasks.)

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

Special Categories of Data

Special category data (formally known as Sensitive Personal Data) is personal data which is more sensitive, and so needs more protection.

Special category data includes information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or sexual orientation

In order to lawfully process special category data, the Academy must have a lawful basis (as set out above) and meet one of the following conditions:

(a) the data subject has given explicit consent[2]
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent

[1] This condition should not generally be used where one of the other basis would be more appropriate.
[2] Except where law provide that the prohibition may not be lifted by the data subject

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
(e) processing relates to personal data which are manifestly made public by the data subject
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
(g) processing is necessary for reasons of substantial public interest
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
(i) processing is necessary for reasons of public interest in the area of public health
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

The Data Protection Officer will advise on which basis the Academy can process special categories personal data.

Criminal Offence Data

Data Protection law requires that the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

The Academy must not process Criminal offence data unless it meets specific terms and conditions. Staff must not process Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer.

Consent

In some cases, the Academy may need to rely on an individual's explicit consent to process their personal data.

Where the Academy is relying on Consent to process personal data it will ensure that:

- Consent is the most appropriate lawful basis for processing
- The request for consent is prominent and separate from other terms and conditions
- We ask people to positively opt in
- We don't use pre-ticked boxes or any other type of default consent
- We use clear, plain language that is easy to understand
- We specify why we want the data and what we're going to do with it
- We give individual ('granular') options to consent separately to different purposes and types of processing
- We name our organisation and any third-party controllers who will be relying on the consent
- We tell individuals they can withdraw their consent
- We ensure that individuals can refuse to consent without detriment
- We avoid making consent a precondition of a service

Consent to Share Special Categories of Data

In some cases, the Academy may need to rely on explicit consent to process personal data.

Example: To assist the school in providing appropriate learning support, we will ask for a parent's explicit permission to share and/or obtain relevant information from the individual and/or outside agencies.

A template consent form is provided at Appendix 7.

If staff wish to share any Special Categories of Data for other purposes they should seek advice from the Data Protection Officer.

Marketing

There are specific rules around sending advertising or marketing material which is directed to specific individuals.[3] Routine service messages do not count as direct marketing – in other words, correspondence to provide information they need about the Academy (e.g. information about college closures due to bad weather, safety announcements, changes to term dates etc.). General branding, logos or straplines in these messages do not count as marketing.

When sending specific marketing message, the Academy must obtain consent to send any emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar electronic messages.

Consent must be obtained in line with the process set out in this Policy. All marketing projects must be approved by the Data Protection Officer and Marketing Department.

Privacy Notices

Data Protection law requires that the Academy provides specific information about what information it is collecting and why, this is called a Privacy Notice.

Privacy Notices must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- free of charge

The Academy has an overarching Privacy Notice on its website which includes:

- Full name and address of the Academy
- Identity and contact details of the Data Protection Officer
- Purpose of the processing and the lawful basis for the processing
- The legitimate interests of the Academy or third party
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority (the ICO)
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data

[3] Privacy and Electronic Communication Regulations / e-Privacy Directive 2018

- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

In some cases, it will be appropriate to include a specific statement on data collection forms used by the Academy. A template statement is provided below. Staff must ensure that they provide the Data Protection Officer a copy of any template data collection forms which include the Privacy Statement so that a central register can be maintained.

Template Privacy Statement
The Oaks Academy collect your [what personal details e.g. name, address, date of birth] so that we can [high level reason for collecting the details].

We collect and use your information [specific reasons for collecting the details].

We will share this personal data with [people/companies we share the data with] for the purpose of [reason]. Your data [will not be sent outside of the UK.] / or [will be transfer to (name of countries)].

We will retain this information in line with the retention timescales set out in our Data Protection Policy.

You have a number of rights under data protection law including the right to be informed, right of access, right to rectification, right to erase, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling.

If you have any questions about the use of your personal data please see our Privacy Notice or contact our Data Protection Officer (dataprotect@ccsw.ac.uk). If you are unhappy with our handling with your personal data, you have the right to make a complaint to the Information Commissioners Office.

Obtaining Personal Data from Third Parties

Where the Academy obtains data not directly from data subject e.g. lists provided by a school of individuals to contact we must also provide specific information. When obtaining personal data from a third-party staff must contact the Data Protection Officer to ensure this can be recorded on the Data Map register and the required Privacy Statement can be drafted.

Publication of Academy Information

It is the policy of the Academy to disclose relevant information to the public; in particular, the following information will be available to the public for inspection:

- names and contact details of Academy governors;
- list of all staff;
- photographs of key staff;
- the information published in accordance with the Academy's publication scheme adopted pursuant to the Freedom of Information Act 2000

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.

Principle 2 – Specific and explicit purposes

This principle aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

In practice, the second data protection principle means that the Academy must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it
- comply with the fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data
- notifying the Information Commissioner of our processing
- ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair

Principle 3 – Adequate, relevant and necessary

The Academy must ensure that all personal data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Staff must ensure that they are only collecting the minimum data for the purpose for which it is required.

Principle 4 – Accurate and up to date

The Academy is required to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all staff who collect and use personal data to take reasonable steps to ensure it is kept up to date as possible.

All data should be held centrally; unnecessary duplicate or additional sets of data should not be created or filed separately. The Academy will prompt parents and staff to update their details.

A template form has been provided in Appendix 6 for parents to submit a change of details.

Principle 5 – Retention

The Academy will ensure that personal data is kept no longer than is necessary.

Records which have reached the end of their life (whether held in electronic or paper format) should generally be destroyed under confidential conditions. Once a document reaches its retention period it should be reviewed to ensure it does not need to be kept for longer as some records need to be kept for historical purposes and these will be transferred to a place of deposit by the Data Protection Officer. Any staff wishing to retain a record for longer than the specified retention period should contact the Data Protection Officer for advice and guidance.

A Document Retention Policy has been produced and staff must review this policy and ensure records are kept in line with the timescales specified. Staff must ensure that once data has reached its retention period it is destroyed securely. All personal data held in paper form must be disposed of by shredding or in the shred bins provided on Academy premises.

Electronic media will be disposed of securely by the IT department.

Principle 6 – Security

The Academy will ensure that data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Appendix 3 – Compliance with Data Subject Rights

The right to be informed

This right is outlined in Appendix 1, see Privacy Notices.

The right of access

Data subjects have the right to access personal data that is currently being kept about them. Any person who wishes to exercise this right should complete the Academy 'Access to Data' form (See Appendix 5) and submit it to the Data Protection Officer.

The Data Protection Officer will log the request on the Academy's SAR database and liaise with the required departments to collate the personal data.

There are some limited exemptions which allow the Academy to withhold certain data (these can only be applied by the Data Protection Officer); however, generally all information should be supplied.

Disclosing personal data (Section 29 Forms)

The Academy is permitted to disclose personal data for the purposes of Crime and taxation. In the event that a section 29 form is received this must be immediately forwarded to the Data Protection Officer for action.

The right to rectification

The right to rectification gives data subjects the right to have personal data rectified if it is inaccurate or incomplete. If a data subject requests the Academy rectify inaccurate or incomplete data, the request must be sent to the Data Protection Officer for review. The Data Protection Officer will liaise with the relevant department to have the data rectified.

If the Academy has disclosed the inaccurate or incomplete personal data to any third parties, the Academy shall inform them of the rectification where possible. The Data Protection Officer shall inform the data subjects about the third parties to whom the data has been disclosed (where appropriate).

The right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable a data subject to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'.

Data subjects have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the data subject withdraws consent
- When the data subject objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The Academy can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes
- the exercise or defence of legal claims

If the Academy has disclosed the personal data in question to third parties, the Academy will inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

Data subjects have a right to 'block' or suppress processing of personal data. When processing is restricted, the Academy is permitted to store the personal data, but not further process it. The Academy will retain enough information about the data subject to ensure that the restriction is respected in future but no further information.

The Academy is required to restrict the processing of personal data in the following circumstances:

- Where a data subject contests the accuracy of the personal data, the organisation restricts the processing until it has verified the accuracy of the personal data
- Where a data subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the organisation is considering whether our legitimate grounds override those of the data subject
- When the processing is identified to be unlawful and the data subject opposes erasure and requests restriction instead
- Where the organisation no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

If the Academy has disclosed the personal data in question to third parties, the College shall inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Academy shall inform data subjects when it lifts a restriction on processing.

The right to data portability

The right to data portability allows data subjects to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided directly to the organisation
- where the processing is based on the individual's consent or for the performance of a contract and
- when processing is carried out by automated means (on a computer)

Where a data subject requests a copy of their personal data in a portable form the Academy will supply the data held in a structured, commonly used and machine-readable form. Generally, this will

be a CSV file from the Academy's computer systems. The information will be provided free of charge.

If the data subject requests it and if it is technically feasible, the Academy shall securely transmit the data directly to another organisation.

If the personal data concerns more than one individual, the Data Protection Officer will consider whether providing the information would prejudice the rights of any other individual.

The right to object

Data Subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics

In the event that an objection to processing is received this should be immediately forwarded to the Data Protection Officer who will consider and where required coordinate the ceasing of processing.

Where a request is received the Academy will stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

Data Protection law includes specific rules where the Academy is conducting automated individual decision-making (making a decision solely by automated means without any human involvement); and/ or profiling (automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements).

Wherever the Academy wishes to use automated decision making and/or profiling the Academy will carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to comply with the law.

Appendix 4 – Guidance on Disclosing / Sharing Personal Data of Students:

Personal data must not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

Requests for information on students may come from:

- Parents/Guardians/Carers
- Other family members, friends etc.
- Potential employers and education institutions - reference requests
- Government Agencies

- Parents / Guardians / Carers

Staff should only discuss students with the parent/carer with parental responsibility. If in doubt always take contact details and then confirm. When receiving calls by phone it is important to take steps to verify the identity of the caller by either asking the caller to verify key data items or by calling the caller back on the phone number listed in the student file.

- Other Family Members, Friends etc

Staff should not respond to any enquiries from other family members or friends and should not even confirm that someone is a student at the Academy. If the reason for the enquiry is stated to be an emergency, then the matter should be referred to the SLT.

- Potential Employers and Education Institutions - Reference Requests

These should be dealt with by the Pastoral Managers and Key Stage Directors. All reference requests and responses should be in writing. The student is entitled to see copies of any reference written about them.

See separate guidelines on the writing of references.

Copies of all references should be kept in the student file.

- Government Agencies

Government agencies can include, but not be limited to the Local Authority, DFE, Social Services, Police, Benefits agencies, probation service, tax etc.

The Academy is legally bound to provide information to various government agencies. All requests for information and all responses should be in writing. Copies of all requests should be kept, preferably in the student file.

Staff should seek advice from the Data Protection Officer when responding to any such requests.

Appendix 5 – Access to Data Request Form

You have the right under Data Protection law to see personal information that we hold about you.

Please complete the details below to enable us to identify you and your information.

Full name (s) (include any previous known names)	
Current address	
Previously known address(s)	
Contact tel. and/or email	
Date of birth(s)	
Student no(s)	
Dates attended	
To help us locate your information quickly please provide as much detail as possible about the type of information required.	
Where the information is held in an electronic form would you like the data provided to you electronically	☐ Yes ☐ No
Data Subject(s) Declaration:	Signed…….. Date……

Please provide two copies of current identification confirming your signature and current address (e.g. passport or driving licence, and utility bill) as in order for your request to be processed. If the information is insufficient or incomplete to action your request the statutory time frame will be suspended, whilst further information is collated from you.

The Academy has a statutory one month (this can be extended by two months where the request is complex) to comply with a Data Subject Access Request, this time frame will only commence when the Academy is in receipt of this form and the required identification documents. Where the timescale is extended the Academy will inform you of any such extension.

Data Subject's Representative

If you are seeking information about someone who is unable to contact the Academy directly please provide the Data Subject's written consent and current identification confirming their signature and current address, or appropriate Court Order or Power of Attorney.

Please complete the details below if you are acting as the representative to the data subject.

Full name/Organisation	
Address	
Relationship to data subject	
Contact tel. no. or email	
Data Subject Representative Declaration: I confirm that I am acting as the data subject's representative and include the appropriate consent document(s) and identification for them. Signed …… Date……..	

Please forward all completed request forms and copies of ID to:

Email: dataprotect@ccsw.ac.uk

Or

Data Protection Officer
Cheshire College - South & West
Crewe Campus
Dane Bank Avenue
Crewe
CW2 8AB

Appendix 6 – Student Details Amendment Form

Additional or Replacement Contact

On the enrolment form, you provided your personal details; however, if these have changed please complete this form and give it to your Form Tutor or the School Office.

Details	Current	Revised
Your name		
Address		
Postcode		
Name of Parent/Guardian/Carer		
Parent/Guardian/Carer Address		
Parent/Guardian/Carer Telephone		
Is this a **replacement** to the original name or an **addition**?		
Your signature		
Date		

Appendix 7 – Student Data Sharing Consent Form

To assist the Academy in providing appropriate learning support, we would ask you to give consent for us to contact and/or obtain relevant information from the individual and/or outside agencies as follows:

- Medical (GPs/Doctors/ Hospital/Clinic)
- Social Services
- Probation Service/Home Office
- Previous School SENCOs/Teachers
- LEA Support Services
- DEA Employment Services
- Voluntary and Community Sector Organisations
- Transport Providers e.g. Bus Service, Taxi Drivers

I give my consent for The Oaks Academy to share and/or obtain information that is relevant to my child's education and support from the individuals/outside agencies indicated above. The information will be kept secure and remain confidential.

Name of Student: ……..……..

Date of Birth: ……

Name of Parent/Carer: ……..……

Signature of Parent/Carer: ……

Date: …….

Appendix 8 – Data Breach Management Process

On receipt of a Data Breach Form the Data Protection Officer shall:

- Record the incident on the Academy data breach database
- Identify who is responsible for managing the incident, investigation and performance – generally a member of SLT
- Agree the grading of the incident SLT members (as per the below)
- Identify and inform key stakeholders
- Inform the Information Commissioners Office and/or data subjects (where required – as below)
- Institute recovery actions e.g. retrieval of the data if possible
- Invoke the Academy's disciplinary procedure as appropriate or document the reasons where it is decided not to take action
- Institute appropriate counter-measures to prevent recurrence including issuing lessons learned communications

Data Breach Grading Criteria:

Near Miss	No personal data at risk nor data to which a duty of confidence is owed, information readily accessible or already in the public domain or information is unlikely to identify individual
Minor	Breach **does not result in a risk** to the rights and freedoms of individuals e.g. Information is lost in a protected format (e.g. encrypted USB stick)
Moderate (ICO reportable)	Breach **results in a risk** to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss (leaves individuals open to identity theft), loss of confidentiality or any other significant economic or social disadvantage.
Severe (ICO reportable) (Reportable to the data subject)	Breach **results in a HIGH risk** to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss (leaves individuals open to identity theft), loss of confidentiality or any other significant economic or social disadvantage.

Notification of the breach

Data Protection law places a duty on the Academy to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the organisation must also inform those individuals without undue delay.

In the following cases the law requires the Academy to notify the ICO and the individuals exposed by a data breach to allow the risks to be mitigated and to protect the individual: Without undue delay and, where feasible, not later than 72 hours after having become aware of it, the organisation must notify the personal data breach to the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Academy shall communicate the personal data breach to the data subject without undue delay.

The structure of the notification to the ICO:

- description of the nature of the personal data breach including, where possible the categories of data and approximate number of individuals concerned
- the name and contact details of the data protection officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

The structure of the notification to an individual (data subject):

- Opening paragraph - take responsibility and apologise
- In clear and plain language explain the nature of the data breach
- Give a description of the likely consequences of the personal data breach
- Give a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects e.g. explain their options
- Provide the name and contact details of the Data Protection Officer
- Invite a discussion with a member of SLT

The Academy may also choose to notify the ICO and the data subjects of breaches that do not meet the above criteria where the notification has a clear benefit e.g. whether this is to enable the individual affected to be given options of different actions the organisation have available to protect them, make an official complaint or to allow the appropriate regulatory bodies to perform their functions and provide advice.

Data Breach/Near Miss Submission Form

Please complete as much information as possible and send the form to dataprotect@ccsw.ac.uk

Date and time of the incident:	
Location of the incident:	
Type of incident e.g. Theft, accidental loss, inappropriate disclosure, procedural failure etc	
Description of what happened:	
Who does the data relate to? E.g. student, parent, staff, visitor, other – please specify	
The number of records/ amount of data involved (approximately)	
The format of the records (paper or digital)	
Which internal individuals have been notified e.g. your line manager, SLT members?	
Is any external party involved? E.g. has the data been sent to a private individual, are the press/media involved?	

Thank you for reporting this incident. The Data Protection Officer will respond as soon as possible with advice and next steps on managing this incident.