DATA PROTECTION POLICY

Data Protection Policy
V2.0
Sarah Otto/September 2024

CONTENTS

At a glance

Oasis is committed to transforming communities in an inclusive way so that all people experience wholeness and fullness of life. This work involves the processing of personal data. We recognise our legal obligations to Data Protection and the obligations we place on ourselves in the context of the Oasis Ethos and Nine Habits.

The central purpose of Oasis is to transform communities so that they are safe and healthy places to be and to live. Oasis realises that it cannot make a commitment of this kind without first being committed to the protection of the personal data that we are responsible for.

Checklist

- ❑ We will protect the rights of individuals for whom we process their personal data.
- ❑ We will implement appropriate technical and organisational security measures against unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- ❑ We will process personal data in accordance with the seven data processing principles.
- ❑ We will be open, honest and transparent about the processing of personal data.
- ❑ We will communicate using clear and plain language which is age appropriate.
- ❑ We shall be responsible for and demonstrate compliance with the UK GDPR.

In brief

This policy defines how Oasis will classify, manage and protect personal data in its control in a clear and transparent manner. The policy covers personal data and sensitive or special category data processed by Oasis.

It sets out the requirements, responsibilities and accountabilities associated with this policy. Failure to adhere to this policy may lead to disciplinary action being taken. Breaches of this policy may be considered misconduct up to and including gross misconduct.

Oasis is committed to protecting the right to privacy of individuals and will process personal data in line with the data protection principles, which means that personal data will be:

i. processed lawfully, fairly and in a transparent manner.
ii. collected for specified, explicit and legitimate purposes and not used for other purposes.
iii. adequate for the requirement, relevant and limited to what is necessary in relation to the purposes for which they are processed.
iv. accurate and, where necessary, kept up to date.

v. retained for the minimum period required to meet Oasis's statutory and legal obligations or for the successful undertaking of Oasis's operations.
vi. kept in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful access and against accidental loss, destruction or damage.

Data Protection

Data Protection (DP)

Oasis is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act (DPA) 2018 and the UK General Data Protection Regulation (UK GDPR).

Oasis needs to collect, retain, and process personal data. This information may relate to staff, students and other individuals including parents/guardians of students, volunteers, donors, visitors, contract staff, and users of Oasis premises. Therefore, Oasis is acting as a Data Controller.

Oasis consists of several different subsidiaries. As Data Controllers, Oasis subsidiaries are registered separately with the UK Data Protection Regulator, the Information Commissioner's Office (ICO). Each subsidiary or legal body will register on behalf of all entities within that subsidiary. For example, Oasis Community Learning (OCL) registration applies to all academies, although each academy will be considered as a separate Oasis entity for the purposes of this policy. All academies will be listed as trading names of OCL. Oasis registration details are published on the ICO website.

All data processing will be carried out in accordance with principles stated earlier in this policy.

The reasons for collecting, processing, transforming, and reporting information includes but is not limited to the following:

- Conduct and administer programmes of study, record progress and agree awards.
- Undertake the administration of Oasis as an organisation e.g.to recruit and pay staff.
- Comply with legal and statutory obligations to funding bodies and government.
- Report on various aspects of educational and other measures.
- Comply with legal requests for information.
- Conduct a wide range of planning & operational activities.
- Fundraise in pursuit of Oasis's objectives.

Data Classification

In order to effectively manage and secure Oasis Data, it is necessary for it to be classified so that it can be handled appropriately. Oasis will categorise data in line with the UK GDPR:

- **Personal data** is data relating to a living individual who can be identified from that information or from that data and other information in possession of Oasis. This includes but is not limited to name, address, telephone number, ID number. This also includes expression of opinion about the individual, and of the intentions of Oasis in respect of that individual. Information about IT usage including IP address is considered as Personal data.

- **Sensitive Data** is different from ordinary personal data (such as name, address, telephone) and includes the definition of special category data used the Data Protection Act 2018. It relates to racial or ethnic origin, political opinions, religion, trade union membership, health, biometrics (where used for ID purposes) sexual orientation and criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Oasis may consider personal data, where its disclosure has wider, significant implications as Sensitive for the purposes of processing. For example, personal data relating to children may be considered as sensitive.

Oasis will implement levels of security and protection for different classifications of data. Further requirements for this are detailed in the Oasis Information Security Policy.

Accountability for Data Protection in Oasis Community Learning

Overall accountability for data protection compliance within Oasis lies with the board of the Oasis subsidiary. In Oasis Community Learning (OCL) accountability for data protection lies with the OCL Board.

The Data Protection Officer (DPO) will advise on and monitor OCL's compliance with the DPA 2018/UK GDPR and act as the organisational contact for the Information Commissioner's Office and for any data subject affected by OCL's data processing.

The DPO is responsible for providing advice and guidance, as required to support data protection compliance within OCL.

The DPO is recognised as the principal expert on Data Protection within OCL and therefore should be contacted to resolve any queries related to this policy or data protection issues. Academy Principals are accountable for ensuring that the policies and processes are adhered to for Academy Data and by Academy Staff.

Each academy will designate local Data Protection Lead with responsibility for liaison with the national DPO and supporting the process of auditing compliance.

It is possible to delegate responsibility to a Data Protection Lead but accountability for Data Protection Compliance is always retained by the academy Principal or National Head of Service.

National Service Leads are accountable for ensuring that the policies and processes are adhered to for nationally held data and by national staff within their service. Heads of National Services may choose to nominate a Data Protection Lead for their service. If they do not do so then the Head of Service themselves will be assumed to be the Data Protection Lead for the service.

The DPO will maintain a record of all Data Protection Leads. The Academy Principal/Head of National Service is responsible for ensuring that the DPO is notified if the Data Protection Lead changes or if the individual occupying the role leaves Oasis Community Learning.

The DPO will be accountable for advising on new policies, maintaining all forms and logs related to subject access requests and data breaches, and data protection related training, as well as identifying requirements for changes and additions. The Deputy Chief Operating Officer will be accountable for the development of data protection policies.

The policy applies to all staff and students of OCL. Compliance with data protection legislation is the responsibility of all members of OCL. OCL has developed a range of policies, processes, standards and guidance relating to data protection, Information Security and IT Security which are detailed earlier in this document and together provide the framework for the effective protection and management of personal data within the organisation.

People who are part of the OCL family, including Volunteers, Staff and Students of OCL (or their Parents & Guardians where appropriate), are responsible for ensuring that any personal data they supply about themselves to OCL is accurate and up to date. If any information supplied changes, they should inform OCL as soon as practical via applicable channels.

Other agencies and individuals working with OCL, and who have access to OCL personal data, must read and comply with this policy. Academy Principals and Heads of National Service are responsible for ensuring that third party organisations, contractors, volunteers and consultants have read and agreed to comply with this policy before they are granted access to any systems containing personal data.

OCL will retain evidence that all individuals who have access to personal data within their control have read and agreed to adhere to this policy.

OCL offers a programme of training to ensure that all individuals processing personal data are familiar with best practice in data protection and information security along with the detail of this policy.

All OCL staff must undertake online computer-based data protection training first upon induction and then annually. Academy Principals are accountable for ensuring that all academy-based staff complete this training annually. National Service Leads are accountable for ensuring that all National Staff complete this training annually.

Those with regular access to significant volumes of personal data must undertake additional face to face or Teams training in data protection before being granted access to systems containing significant personal data.

All those with access to sensitive data or special category data must undertake additional face to face training in data protection before being granted access to systems containing significant sensitive or special category data.

Academy Principals and National Heads of Service are accountable for ensuring that systems containing personal data that are within their area's responsibility adhere to this policy.

Management of Personally Identifiable Information

Oasis will process minimum amount of personal data possible for the successful operation of the organisation and to comply with the organisation's legal and statutory obligations.

All Personally Identifiable Information Controlled by Oasis will have a named individual as the Data Owner. The Data Owner has responsibility for the data delegated to them by the individual responsible for the Oasis Entity controlling the data.

The personal data stored may be retained within Oasis systems or within systems managed by third parties acting as Data Processors. Regardless of the storage location, an Oasis Data Owner will be identified.

The Data Owner should be someone who has knowledge of the data and its purpose. The Data Owner will not be a member of the Oasis IT Services Team unless the personal data is related to members of the Oasis IT Services team themselves.

The Data Owner should seek to minimise the data held.

The Data Owner will have responsibility for determining the basis for processing, how long the data should be retained for and who should have access to the data. The information around the data will be documented on our record of processing activities (ROPA). Guidance on the production of our ROPA and a standard Template for this is available in the Guidance for the Collection and Cataloguing of Personal Data located on the policy portal.

All personal data processed by Oasis must be catalogued and the basis for the processing documented. The Oasis leader of each Oasis Entity is accountable for ensuring that all data within their sphere of responsibility has been catalogued and the basis for processing has been recorded.

Whilst other individuals or departments may have responsibility for facilitating the storage and access to personal data, determination of what should be stored, for how long and who should have access to it lies with the Data Owner. For example, a member of the Property and Estates team may be responsible for issuing the keys to the filing cabinet that contains the personal data, but it is the Data Owner who would determine who should be issued with a key.

OCL's Privacy notice is available on our website and should also be made available to data subjects on request. Privacy Notices should be easy to understand and appropriate for their audience including using age-appropriate language.

Oasis Entities manage systems and business processes that involve the processing of personal information. The responsible Oasis Entity must develop and document policies and procedures for the safe and secure handling of personal information for approval by the DPO and the relevant board. Ownership of individual systems and business processes is detailed in Appendix 2 of this document.

The processing of Sensitive or Special Category Data requires additional precautions to be taken to ensure its safe processing. Details of appropriate security measures are detailed in the Oasis Information Security Policy and IT Security Policy.

Oasis Entities will identify where they consider data to be classified as sensitive in their data catalogue.

Oasis Entities will record details of those employees with access to sensitive personal data.

Controls within Oasis Community Learning

The Data Protection Lead at each academy will undertake regular checks of compliance with the UK GDPR under the direction of the principal or in accordance with national initiatives to be advised from time to time.

The DPO or a designated suitably experienced colleague working to the DPO will undertake data protection audits. The DPO may choose at their own discretion to undertake an OCL audit for whatever reason but particularly this may be in response to any Data Protection related concerns raised or Data breaches reported. The regular programme of DPO audits will be notified to the board's Audit and Risk Committee.

The DPO will provide a report to the Audit and Risk Committee of the OCL board as to the status of data protection compliance and data protection risk in OCL in advance of each Audit and Risk Committee meeting. The report shall not be subject to any alteration by anyone other than the DPO.

Alteration of the DPO board report or attempting to unduly influence its contents will be considered to be a disciplinary offence.

Consideration of the Data Protection Compliance and Risk Report will be a standing agenda item for the Audit and Risk Committee of the OCL Board.

Any member of the OCL Board may request an extra-ordinary Data Protection Report at any time from the DPO.

Impact Assessments / Risk Assessments

Decisions around the processing of personal data within Oasis will be undertaken with suitable regard for the risk and impact to the privacy and rights of data subjects before processing is undertaken.

Data Protection Impact Assessments will be undertaken when a new business process or processing activity is likely to result in a high risk to the rights and freedoms of data subjects.

Data Protection Impact Assessments will be undertaken by staff who are suitably trained to undertake them. They must consult with the DPO at an early stage in the process and receive sign off from the DPO when the Data Protection Impact Assessment is completed. All such final assessments must be held by the DPO on behalf of OCL.

The Data Protection Impact Assessment will be undertaken using the guidance and templates provided in the OCL Data Protection Impact Assessment Procedure.

The results of the Data Protection Impact Assessments will be retained by the DPO and the Academy or National Service undertaking the assessment for inspection at any time.

Data Protection Breaches

A Data Protection Breach is where personal data is lost, stolen and/or accidentally becomes available to those who are not authorised to have access to it.

Oasis will report all notifiable data protection breaches to the ICO and only the DPO can contact the ICO on behalf of OCL.

Data Protection breaches must be reported using the Oasis Data Protection Breach Reporting Process.

Any individual who becomes aware or suspects a Data Protection breach must inform the DPO immediately regardless of the severity or the perceived severity of the breach. Failure to notify the DPO of a breach immediately may lead to disciplinary action.

Procurement

Data Protection issues must be considered at the point of procurement where goods or services being procured have an impact on Data Protection and involve the handling of personal data. Where a supplier will also process personal data on behalf of OCL, the OCL data sharing agreement template should be used. The data agreement template is on the data protection national portal.

Data Protection Impact Assessments (DPIAs) as outlined in the OCL DPIA procedure will be undertaken in regard to the procurement of any particular goods or services for the first time where Personal Information is involved.

Before a new supplier can be involved in the processing of OCL's personal data, a contract must exist which sets out the obligations and requirements of the supplier to the processing of this data. The supplier must be subject to appropriate due diligence in regard to their data protection practices guaranteeing that they will implement appropriate technical and organisational measures to meet UK GDPR requirements.

Oasis will maintain a register of organisations whose data protection practices have been verified and approved and a record of the contract that is in place.

Oasis Entities who procure services that involve the processing of Oasis' personal data must ensure that appropriate contract terms are included in any agreement with the supplier to ensure that Oasis' data is appropriately managed. Guidance on appropriate Data Protection contract terms can be obtained from the DPO.

Data Subject Rights

Oasis respects the rights of data subjects to access the data that Oasis processes about them. For further information, please refer to the subject access request (SAR) policy.

Data Subjects have specific rights regarding the processing of their personal data and these rights include:

- To make a SAR regarding the information held and to whom it has been disclosed.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision-making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Data Protection Act.
- To request the Information Commissioner's Office (ICO) to assess whether any provision of the Act has been contravened.

Oasis Entities need to have in place effective means of extracting and retrieving information from a variety of sources in order to comply with a subject access request. Oasis will manage and respond to subject access requests in accordance with the Oasis Subject Access Request Policy.

Lawful Processing and Consent

All Data Processing undertaken by Oasis must be lawful.

It is only lawful to undertake the Processing of personal data on the following basis:

- With the explicit consent of the data subject.
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of a data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. This condition is not available to processing carried out by public authorities in the performance of their tasks. Where another basis for processing personal data does not exist, personal data or sensitive personal data can only be obtained, held, used or disclosed with the explicit consent of the data subject. "Consent" means that the data subject or an appropriate parent/legal guardian has been fully informed of the explicit intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. The subject/parent/guardian must give consent freely of their own accord.

For further details on consent please refer to later section on Consent.

Security of Electronic Data

The Oasis IT Security Policy sets out the requirements for the secure handling and management of electronic data which has a significant impact on Data Protection, and secure use of IT systems which has a significant impact on data protection. All Oasis staff are responsible for ensuring that they are familiar with and comply with this policy at all times.

Access to personal data should be limited to those who need to access it in undertaking their legitimate duties as part of Oasis.

Security of Hard Copy (Paper Based) Data

The Oasis Information Security Policy sets out the requirements for the secure handling and management of information which has a significant impact on data protection. All Oasis staff are responsible for ensuring that they are familiar with and comply with this policy at all times.

Authorised individuals are individually responsible for the 'Hard Copy' personal data in their care.

'Hard Copy' paper based personal data should be secured with access restricted to those with legitimate access requirement.

'Hard Copy' personal data must be recorded in the data catalogue along with electronic data.

Retention and Disposal of Data

Personal data should not be retained for any longer than this is required for the lawful processing of the data. Once the data is no longer required for a specific purpose, then it must be disposed of in a way that protects the rights and privacy of data subjects.

Hard copy of personal data must be disposed through secure waste disposal. Guidance on the secure deletion/disposal of electronic information is available in the Oasis Information Security Policy.

There are a range of different legal and statutory obligations requiring the retention of information that impact Oasis activities as a Data Controller. Personal data must be retained in accordance with the Oasis Data Retention Policy to ensure that these obligations are met.

Routine Publication of Information

Oasis publishes a number of items that include personal data and will continue to do so. The following is an indicative list:

- Names of all Oasis Trustees including members of Oasis Committees, Boards and other current and future Governance forums.
- Names, job titles and academic and/or professional qualifications of members of staff.
- Awards and Honours including Prize winners.
- Internal Telephone Directory.
- Graduation programmes and videos or other multimedia versions of graduation, award and other ceremonies.
- Information in prospectuses (including photographs), brochures, annual & other reports, staff newsletters, etc.
- Staff information on Oasis website including photographs.

It is recognised that there might be occasions when a member of staff, a student, or a lay member of Oasis, requests that their personal details in some of these categories remain confidential or are restricted to internal access. The individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, Oasis should endeavour to comply with the request where possible and ensure that appropriate action is taken. However, where the information is published for regulatory reasons or where the information is published because of a legal obligation, then the information will continue to be published.

Communications and Marketing

Oasis requires **explicit consent** for direct marketing activities. Marketing Activities can include both direct communications with those who have parental responsibility and to members of the wider community.

Marketing activities are distinct from communications which are as a result of a child being part of Oasis. For example, information about a change in academy policy being sent home in a letter or an SMS message advising parents that the academy is closed due to bad weather is not marketing activity, information about an optional event being hosted at the academy could be considered marketing activity.

In order to ensure compliance with the regulation, academies must maintain separate 'lists' of contact information to be used for different communication purposes in the systems that are deployed. For example, a list in the text messaging service for 'All Parents' and a list in the text messaging service for 'Marketing to Parents' that corresponds to the consent received.

CCTV

Oasis makes use of CCTV. The use and management must be undertaken in compliance with the Oasis CCTV policy.

Disclosure of Personally Identifiable Information

Oasis will only disclose Personal Information in its control in accordance with this Policy.

Safeguarding

Oasis has a need to process Sensitive or Special Category data relating to its Safeguarding obligations.

Safeguarding requirements and the management of Safeguarding related Personal Information must be managed in accordance with the provisions of this and the related Oasis policies.

Transfers of Data between Oasis Subsidiaries

Oasis entities that form part of the same legal subsidiary may share personal information where required and in compliance with this and other Oasis policies.

Oasis is an organisation made up of different legal bodies. Data transfers between the legal bodies represents a transfer between organisations and will only be undertaken when a Data Sharing Agreement is in place between the legal bodies.

Oasis UK will not transfer personal data to another Oasis Subsidiary or Organisation outside of the UK for any purpose unless the transfer complies with any applicable cross border transfer requirements.

Data Protection Consent as a Lawful Basis of Processing

Very little of our processing of personal data is covered by the lawful basis of “consent”. That is because under “public task” we do not need data subjects’ prior agreement to process their personal data. Consent can be provided in a range of forms including verbal, electronic and written consent. 'Opt-outs' and 'implied consent' will not be used, and all consent must require a positive selection or choice to opt in. So pre-selected options must not be used. Where verbal consent is obtained then records of the consent must be maintained.

In most instances Oasis will process data on a legal basis other than consent. Where consent is used as the legal basis of processing then explicit consent will be obtained before any processing is undertaken. Any Oasis forms (whether electronic or paper-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom the information may be disclosed. Separate consent is required for each separate processing activity and usage of the data where consent is used as the legal basis of processing. If an individual does not consent to certain types of processing (e.g., direct marketing), appropriate action must be taken to ensure that the processing does not take place.

The list below shows the main activities within Oasis which fall under the lawful basis of “consent” because they fall outside our statutory responsibilities. Consent must be obtained in writing for those activities and entered in Bromcom where it relates to students, and a copy of the written consent must be retained in line with OCL’s

Retention Policy. The list is non-exhaustive. Any other activities may need bespoke consent. Appendix 3 shows a sample consent form which can be adapted. If you need to obtain bespoke consent the section below explains what you need to consider.

For students aged under 13 or who lack mental capacity, the parent's consent is required. For students aged 13 or over, the student's consent is required. In some cases, parental consent is also necessary, even when the student is over 13. There is no set time limit for consent. How long it lasts will depend on the context. However, consent should not be maintained for longer than three years, we aim to refresh consent annually.

Some activities require "permission" rather than "consent". The difference is that some activities need prior explicit agreement but have nothing to do with data protection or the processing of personal data. An example is parental agreement to a student going on a trip or visit – a "permission".

Oasis will respect the rights of children as data subjects to make informed consent where they are judged to be able to do so. In most circumstances, this will be considered when children are 13 years old. However, it may be appropriate to consult the person with parental authority where the child may not be fully competent to understand the implications of their decisions.

List of activities requiring parental/carer consent:

- To use images of the student within the academy (banners, plasma screens, displays, etc.) (photographs, video).
- To use images of the student in academy external print publications, e.g. academy prospectus.
- To use images of the student on academy website (photographs, video).
- To use images of the student in academy newsletter (emailed to parents and published on website).
- To use images of the student on academy social media (photographs, video).
- To release personal data (name, images) to local or national media (academy or Oasis national team).
- To process the student's biometric data (e.g. catering).
- To receive marketing information about events in the academy, the hub and the local community.
- To receive information from Oasis about its work in the UK and worldwide.
- To use images of the student within the Oasis national office (banners, plasma screens, displays, etc.) (photographs, video).
- To use images of the student in Oasis national internal and external print publications.

- To use images of the student on Oasis national website (including photographs, video).
- To use images of the student on Oasis national social media (photographs, video).

List of activities requiring student's consent if aged 13 or over:
(In secondary schools, the student's own consent must be given in addition to their parent's, where the student is aged 13 or above.)

- To use my image within the academy (banners, plasma screens, displays, etc.) (photographs, video).
- To use my image in academy external print publications, e.g. academy prospectus.
- To use my image on academy website (photographs, video).
- To use my image in academy newsletter (emailed to parents and published on website).
- To use my image on academy social media (photographs, video).
- To release my personal data (name, images) to local or national media (academy or Oasis national team).
- To process my biometric data (e.g. catering).
- To receive marketing information about events in the academy, the hub and the local community.
- To receive information from Oasis about its work in the UK and worldwide.
- To use my image within the Oasis national office (banners, plasma screens, displays, etc.) (photographs, video).
- To use my image in Oasis national internal and external print publications e.g. Governance Explained Handbook.
- To use my image on Oasis national website (including photographs, video).
- To use my image on Oasis national social media (photographs, video).

Where the processing is related to preventative or counselling services offered directly to a child, then consent can be provided by younger children themselves. Parental/guardian consent is not required in these circumstances.

For Sensitive Data, explicit written consent of data subjects must be obtained unless an alternative lawful basis for processing exists.

Recording Data Protection Consent in Bromcom

The expectation is that academies will make use of the Bromcom MIS system to record data protection consent. There are specific fields that correspond to the consent types above that should be used to record the consent in these areas. It is important that the

specific consent fields provided are used so that standard reports etc can be shared between academies.

Where an academy wishes to record a permission that does not relate to a data protection issue, this should be recorded in the specific field associated with it in the system or in a user defined field and not by adding in an additional data protection consent type.

Requirements for Data Protection Consent

The GPDR sets out some specific requirements when you are gaining consent. These can be broadly summarised as:

- **Unbundled**: Consent must be separate from other terms and conditions. It is therefore important to separate out things that you are asking consent for and data that you are processing on another legal basis. Good practice would be to format a document in such a way as it is clear where consent is being obtained.
- **Active opt-in**: Data Subjects must undertake a positive act to provide the consent. Pre-ticked opt-in boxes are not acceptable. Unticked opt-in boxes or similar active opt-in methods should be used. It is never acceptable to assume consent where it is required so you must not use an opt out.
- **Granular**: Consent for different processing activities and scenarios must be given separately.
- **Named**: Organisations and any third parties who will rely on consent should be named. It means that if you pass the information processed on the basis of consent to another organisation you must include details of who they are when gaining the consent. Categories of third-party organisations are not allowed.
- **Easy to withdraw**: Consent can be withdrawn at any time. If consent is withdrawn, then any data held on the basis of consent must be deleted/removed immediately. It should be clearly stated that users/people have the right to withdraw consent at any time, and you should specify how they can do this. It must be as easy for users to withdraw as it was to give consent.
- **Freely Given**: Consent should not be a precondition of providing a service so it means that anything that you require students and staff to do cannot be carried out on the basis of consent.
- **Documented:** Consent can be given verbally, but it must be documented.

Responsibilities

This policy sets out the requirements, responsibilities and accountabilities associated with this policy. Failure to adhere to this policy may lead to disciplinary action being

taken. Breaches of this policy may be considered misconduct up to and including gross misconduct.

This policy is maintained by the OCL Data Compliance team. Requests to change the policy should be made to the Data Protection Officer.

Training requirements

Details of Data Protection training requirements are set out in this policy.

This policy applies to the following Oasis Entities:

- Oasis Community Learning (OCL)
  - The Oasis Community Learning National Office
  - All Oasis Community Learning Academies
  - All Oasis Community Learning National Services

- Oasis Community Partnerships (OCP)
  - The Oasis Community Partnerships National Office
  - All Oasis Community Partnerships Hub Charities

- Oasis IT Services Ltd
- The Oasis Charitable Trust
- The Oasis Foundation

The policy covers the processing of personal data within Oasis control but is particularly focused on Personally Identifiable Information (Personal Data) which means all activities relating to the processing of data about any living individual.

This includes Personal Data that is stored either electronically or in a relevant filing system.

This policy should be read in conjunction with the following policies:

- The Oasis IT Access Policy
- The Oasis Use of Technologies Policy
- The Oasis IT Security Policy
- The Oasis Information Security Policy
- The Oasis Subject Access Request Policy
- The Oasis CCTV Policy

This policy should be read in conjunction with the following Oasis IT Services Standards:

- The Oasis Device Event Log Configuration Standard
- The Oasis Server Event Log Configuration Standard

This policy should be read in conjunction with the following Oasis IT Services Processes:

- The Oasis Subject Access Request Process
- The Oasis Change Management Process
- The Oasis Data Breach Reporting Process

Statutory requirements

The policy is created with reference to the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

RACI Matrix

"R" is for anyone who is "Responsible" for a task listed in the policy, an "A" is for anyone who is "Accountable", a "C" is for anyone who must be "Consulted" under the policy and "I" is for anyone who must be "Informed" about aspects of the policy.

Policy Element		Leadership			Academy / National			IT	Information Governance
	Board	OCL CEO	OCL COO	Regional Director	Academy Principal / Service Director	Academy Data Protection Lead	Academy / National staff	Director of IT	Data Protection Officer
We will protect the rights of individuals for whom we process their personal data.	A	R	R	R	R	I	I	R/C	R/C
We will implement appropriate technical and organisational and security measures against unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.		A		R	R			R/C	R/C
We shall be responsible for and demonstrate compliance with the UK GDPR.	A	R						C	R/C
We will process personal data in accordance with the seven data processing principles.	A	R	R	R	R	I	I	C	R/C
We will be open, honest and transparent about the processing of personal data.		A			R	R	R	C	R/C
We will communicate using clear and plain language which is age appropriate.		A		C	C				R/C

Appendix 1: Definitions

This section includes the definitions of terms used within this document.

Academy Data:	This refers to all data residing within each academy. IT relates to both student and Academy Staff data. It includes data which is stored within the Oasis IT Services IT System.
Confidential Data:	Confidential Data is information which is held by Oasis which does not relate to a living individual but that it may be damaging to Oasis if access was obtained to the data by someone who was not authorised to access it. An example of this would be financial information such as commercial contractual data.
Data:	For the purposes of this document, Data is any information processed by Oasis. Oasis classifies data into the four categories: General Data, Confidential Data, Personal data and Sensitive Data.
Data Controller:	The organisation that is responsible for the Data. For the purposes of this policy, Oasis Subsidiary or Legal Body is the Data Controller.
Data Processing:	See *Processing.*
Data Subject:	Any natural person who is the subject of Personally Identifiable Information held by Oasis.
General Data:	Data which Oasis holds that is neither personally identifiable nor sensitive. For example, records of the last time that a building was painted or the count of attendance at an Oasis event.
Nationally Held Data:	This refers to all data that is held within National or Central systems relating to National Staff and National Oasis Operations. This includes data relating to Finance, HR, IT and National Procurement. This also includes all data for Governance, Planning, audits and risk.
Oasis Entity:	Oasis Entities are business units that make up the Oasis family in the UK and are either part of Oasis Subsidiaries or subsidiaries in their own right. Oasis Entities include Oasis Academies, Oasis Community Learning National Services, Oasis Community Partnerships Hub Charities. Entities may be separate legal entities or part of a subsidiary that is the Legal Entity.
Personal data:	Data relating to a natural person who can be identified from that information or from that data and other information in possession of Oasis. This includes but is not limited to name, address, telephone number, ID number. This also includes expression of opinion about the individual, and of the intentions of Oasis in respect of that individual. Information about IT usage including IP address should be considered as Personal data.
.	
Personal Data:	Is a general collective term to include Personal or Sensitive Data.
Processing:	Any operation related to organisation, retrieval, disclosure and deletion of data and includes Obtaining and recording data, Accessing, altering, adding to, merging, deleting data Retrieval,

	consultation or use of data Disclosure or otherwise making available of data.
Relevant Filing System:	Any hard copy paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.
Sensitive Data:	Oasis terminology for Special Category Data as defined in the Data Protection Act 2018. It is different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religion, Biometrics (where used for identification) trade union membership, health, sexual orientation, criminal convictions. OCL's handling of sensitive data is subject to much stricter conditions of processing. Oasis may consider personal data, where its inappropriate disclosure has wider implications as sensitive even where it would not be fall into the Special Category Definition.
Third Party:	Any individual/organisation other than the data subject, Oasis or its agents.

Appendix 2: Systems & Business Process Ownership

System	Platform Management	Access Management	Data
Bromcom, CPOMs, MCAS	IT Services	Academy	Academy
iTrent	People Directorate Payroll, Pensions and Compliance	People Directorate Payroll, Pensions and Compliance	People Directorate Payroll, Pensions and Compliance
Dynamic 365 Finance and operations	IT Services	IT Services	Finance Department
File Services (Academy)	IT Services	IT Services	Academy
File Services (National Service)	IT Services	IT Services	National Service

Appendix 3: Standard wording to be used for consent

To be included where consent is being sought from the parent:

To be completed by Parent/Guardian

The Academy would like to seek your consent for the following:

<Insert Consent Causes>

By providing the information in the consent section of this form you give permission for OCL to use the information for the purposes specified. OCL will not use this information for other purposes or pass the information to other organisations without seeking consent from you, or unless we are legally compelled to do so. You can choose to withdraw this consent at any time by contacting the Academy on:

Email: Address:

We will seek to refresh this consent from time to time to ensure that you are still happy for us to process this information. If we do not refresh your consent within three years of the date of this consent then we will delete this data.

Signed: Date:

Print:

To be included where consent is being sought from the student:

To be completed by the student

The academy would like your permission to do the things that are described below. It is your choice whether you allow the academy to do the things which are described below and if you do not want us to then it is ok not to complete this part of the form. You will not get into trouble and it will not affect anything else that happens at school. If you are not sure about anything that is described below then please talk to: <INSERT APPROPRIATE CONTACT> and they will be able to explain it to you.

<Insert Consent Causes using age appropriate language>

By providing the information in this section of this form you give consent for the Academy to use the information for the reasons explained. The Academy will not give this information to anyone else unless we are forced to by law. You can change your mind about this at any time by contacting:
<INSERT APPROPRIATE CONTACT>. We might ask you again if you are still happy for us to carry on doing the things that you have given your consent for, but we will only carry on doing this for three years. If you don't give us consent again after three years, we will delete the information. You can find out more about what we do with your information by looking on the Academy website or by contacting reception.

Signed: Date:

Print:

To be included where consent is being sought on behalf of the student:

To be completed by Parent/Guardian

Due to the age of your child, the Academy would like to seek your consent on their behalf for the following:

<Insert Consent Causes>

By providing the information in the consent section of this form you give consent on behalf of your child for OCL to use the information for the purposes specified. OCL will not use this information for other purposes or pass the information to other organisations without regaining consent from you, or unless we are legally compelled to do so. You can choose to withdraw this consent at any time by contacting the academy on:

Email: Address:

When your child is able to make decisions about the use of the information set out in this section of the form then we will need to seek their consent directly to continue processing this information. At which point we will stop processing the information on the basis of your consent. We will seek to refresh your consent from time to time to ensure that you are still happy for us to process this information on behalf of your child. If we do refresh your consent within three years of the date of this consent, then we will delete this data.

Signed: Date:

Print:

Below you can grant consent for Oasis Community Learning (OCL; the trust your school is part of) to use the information for the purposes specified. OCL will not use this information for other purposes or pass the information to other organisations without seeking further permissions from you, or unless we are legally compelled to do so. You can choose to withdraw this consent at any time by contacting the school.

Please indicate Yes or No to the following fields for data consent:

To use images of the student within the school	Yes / No
To use images of the student in the school external print publications (such as prospectus)	Yes / No
To use images of the student on school website	Yes / No
To use images of the student in the school newsletter	Yes / No
To use images of the student on school social media	Yes / No
To release personal data to local or national media (e.g. student name on a news story)	Yes / No
To receive marketing information about events in the school, hub and community	Yes / No
To receive information from Oasis about its work in the UK and worldwide	Yes / No
To use images of the student within the Oasis national office	Yes / No
To use images of the student in Oasis internal and external print (e.g. a branded document or information brochure)	Yes / No
To use images of the student on Oasis national website	Yes / No
To use images of the student on Oasis national social media	Yes / No

Document Control

Changes History

Version	Date	Owned and Amended by	Recipients	Purpose
V0.1-0.9	Oct 2017	Amended by Shalin Chanchani	Rob Lamont, Steve Hobbs, IT Policy Working Group	Initial drafts for review
V1.0	Dec 2017	Amended by Director of IT & Information Governance, Rob Lamont	COO, John Barneby and OCP & OCT	Draft for Approval
V1.1	June 2018	Amended by Data Protection Officer, Sarah Otto	OCL	Revised by DPO
V1.2	January 2019	Amended by Director of IT & Information Governance, Rob Lamont	OCL	Following Feedback from Head of Compliance, Sarah Graham
V1.3	March 2019	Amended by Director of IT & Information Governance, Rob Lamont	CSG	For Approval Following Feedback
V1.31	April 2019	Amended by Director of IT & Information Governance, Rob Lamont	OCL	Version for Release
V1.32	Nov 2019	Updated wording of 14.1.1 following review	OCL	Version for Release
V2.0	September 2024	Amended by Data Protection Officer, Sarah Otto	OCL	Revised by DPO

Policy Tier

☒ Tier 1
☐ Tier 2
☐ Tier 3
☐ Tier 4

Owner

Sarah Otto

Contact in case of query

Sarah Otto, Data Protection Officer, sarah.otto@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version

Position with the Unions

Does the policy or changes to the policy require consultation with the National Unions under our recognition agreement?

☐ Yes
☒ No

If yes, the policy status is:
☐ Consulted with Unions and Approved
☐ Fully consulted (completed) but not agreed with Unions but Approved by OCL
☐ Currently under Consultation with Unions
☐ Awaiting Consultation with Unions

Date & Record of Next Union Review
Not applicable / Insert

Location
Tick all that apply:
☒ OCL website
☒ Academy website
☒ Policy portal
☐ Other: state

Customisation
☒ OCL policy
☐ OCL with an attachment for each academy to complete regarding local arrangements
☐ Academy policy
☐ Policy is included in principals' annual compliance declaration

Distribution

This document has been distributed to:

Name	Position	Date	Version
OCL Policy Portal			
All staff, via Academies Bulletin			