DATA PROTECTION POLICY

NOVEMBER 2019

CONTENTS

Introduction

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

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 safeguarding and safekeeping of the data that we are responsible for.

a. Purpose

This policy defines how Oasis will Classify, Manage and Protect data in its control in a clear and transparent manner. The policy covers all data processed by Oasis including General data, Confidential Data, Personal Data and Sensitive data.

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.

From time to time, we may amend this policy, so please check back when you next visit this site. Requests to change the policy should be made to the Data Protection Officer.

The objectives of this policy are to:

- Define how Personally Identifiable Information (PII) will be managed within Oasis in accordance with the above principles.
- Define who is responsible for the management of PII.
- Detail the guidance and processes that should be used in the processing of PII.

b. Policy Scope

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

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

c. Policy Principles

Oasis is committed to protecting the right to privacy of individuals and will conduct processing of PII in line with the data protection principles; which means that the 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. processed 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. in a manner that ensures appropriate security of the PII, including protection against unauthorised or unlawful access and against accidental loss, destruction or damage.

d. Related Oasis Policies, Standards and Processes

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 IT Major Investigation Policy
- The Oasis Confidentiality Policy
- The Oasis Password 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
- The Oasis Policy Central Enterprise 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

e. Applicable Legislation, Guidance and References

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

f. Changes to this policy

This policy will be reviewed every year, or when significant changes occur in related legislation or in our strategy. When this happens, we will place an updated version on this document and the date the page has been amended will be visible at the bottom of this page.

Definitions

This section includes the definitions of terms used within this document. A full glossary IT Policy Terms is available as a separate 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.

Personally Identifiable Information (PII):

Is a general collective term to include either 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 in appropriate 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.

Policy Statements

1. Data Protection (DP)

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

1.2. Oasis needs to collect, retain and process a variety of Personally Identifiable Information (PII). 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.

1.3. Oasis consists of a number of different subsidiaries. As Data Controllers, Oasis subsidiaries are registered separately with the UK Data Protection Regulator, the Information Commissioners Office (ICO). Each subsidiary or legal body, will register on behalf of all entities within that subsidiary. For example; the 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.

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

1.5. The reason for collection, processing, transforming and reporting information includes but is not limited to the following:

1.5.1. Conduct and administer programmes of study, record progress and agree awards.

1.5.2. Undertake the administration of Oasis as an organisation e.g.to recruit and pay staff.

1.5.3. Comply with legal and statutory obligations to funding bodies and government.

1.5.4. Report on various aspects of educational and other measures.

1.5.5. Comply with legal requests for information.

1.5.6. Conduct a wide range of planning operational activities.

1.5.7. Fund raise in pursuit of Oasis's objectives.

2. Data Classification

2.1. In order to be able 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 into four different categories:

2.1.1. **General Data** is data which Oasis holds that is neither personally identifiable nor sensitive or special category data. For example, records of the last time that a building was painted or the count of attendance at an Oasis event.

2.1.2. **Confidential Data** is information which is held by Oasis which does not relate to a natural person but it may be damaging to Oasis if unauthorised access was obtained. An example of this would be financial information such as commercial contractual data.

2.1.3. **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.

2.1.4. **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.

2.1.5. Oasis may consider Personal Data, where its disclosure has wider, significant implications as Sensitive for the purposes of processing. For example, Personal Data around children may be considered as Sensitive.

2.2. 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.

3. Accountability for Data Protection in Oasis Community Learning

3.1. 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.

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

3.3. The DPO is responsible for providing advice and guidance, as required to support Data Protection compliance with Oasis Community Learning.

3.4. 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.

3.5. Academy Principals are accountable for ensuring that the policies and processes are adhered to for Academy Data and by Academy Staff.

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

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

3.8. 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.

3.9. 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.

3.10. 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 Director of Information Technology will be accountable for the development of Data Protection Policies.

3.11. 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 data within the organisation.

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

3.13. Other agencies and individuals working with OCL, and who have access to OCL controlled PII, 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 PII.

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

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

3.16. 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.

3.17. Those with regular access to significant volumes of Personal Data must undertake additional face to face training in Data Protection before being granted access to systems containing significant Personal Data.

3.18. All those with access to Sensitive Data and Special Category Data must undertake additional face to face training in Data Protection before being granted access to systems containing significant Sensitive and Special Category Data.

3.19. Academy Principals and National Heads of Service are accountable for ensuring that systems containing PII that are within their areas responsibility adhere to this policy.

4. Management of Personally Identifiable Information

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

4.2. 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.

4.3. The PII being 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.

4.4. 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 PII is related to members of the Oasis IT Services team themselves.

4.5. The Data Owner for a particular piece or pieces of PII should seek to minimize the data held.

4.6. 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[1]. The information around

[1] Guidance for conducting this exercise is available within Guidance for the collection and cataloguing personal data / PII.

the data will be recorded in a 'Data Catalogue' that will be retained for each Oasis Entity. Guidance on the production of a Data Catalogue and a standard Template for this is available in Personal Data Collection and Cataloguing Guidance.

4.7. All PII 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.

4.8. Whilst other individuals or departments may have responsibility for facilitating the storage and access to PII, 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 but it is the Data Owner who would determine who should be issued with a key.

4.9. Oasis Nationally and each Oasis Entity individually must produce and update as is necessary a Privacy Notice to detail the processing of PII. Privacy notice must be published on the Oasis Entity's website and should be available to data subjects on request.

4.10. Privacy Notices should be easy to understand and appropriate for their audience including using age appropriate language.

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

4.12. The processing of Sensitive and 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.

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

4.14. Oasis Entities will record details of those employees with access to Sensitive Data.

5. Controls within Oasis Community Learning

5.1. The Data Protection Lead at each academy will undertake regular checks of compliance with GDPR under the direction of the principal or in accordance with national initiatives to be advised from time to time. The results of the audit must be supplied to the DPO for all nationally-agreed initiatives.

5.2. 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.

5.3. 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.

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

5.5. 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.

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

6. Impact Assessments / Risk Assessments

6.1. Decisions around the processing of personally identifiable 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.

6.2. Data Protection Impact Assessments will be undertaken when a new business process or processing activity is developed that involves the use of Personally Identifiable Information.

6.3. 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.

6.4. The Data Protection Impact Assessment will be undertaken using the guidance and templates provided in the Guidance for the collection and cataloguing of Personal Data.

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

6.6. A copy of the assessment will also be provided to the DPO.

7. Data Protection Breaches

7.1. Data Protection Breach is where PII is lost, stolen, accidentally becomes available to those who are not authorised to have access to it.

7.2. Oasis will report all notifiable Data Protection breaches to the ICO.

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

7.4. 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.

8. Procurement

8.1. Data Protection Issues must be considered at the point of procurement where the good or services being procured have an impact on Data Protection and involve the handling of Personally Identifiable Information.

8.2. Data Protection Impact Assessments as outlined in the 'Guidance in conducting a Data Protection Impact Assessment' will be undertaken in regard to the procurement of any particular goods or services for the first time where Personally Identifiable Information is involved.

8.3. Before a new supplier can be involved in the processing of Oasis Personally Identifiable Information, 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 as outlined in the Oasis Assessment of Third-Party Suppliers Data Protection Practice Process.

8.4. 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.

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

9. Data Subject Rights

9.1. Oasis respects the rights of data subjects to access the data that Oasis Processes about them.

9.2. Data Subjects have specific rights regarding the processing of Personally Identifiable Information being processed by Oasis:

9.2.1. To make a Subject Access Request (SAR) regarding the content and nature of information held and to whom it has been disclosed.

9.2.2. To prevent processing for purposes of direct marketing.

9.2.3. To be informed about mechanics of automated decision-making process that will significantly affect them.

9.2.4. Not to have significant decisions that will affect them taken solely by automated process.

9.2.5. To sue for compensation if they suffer damage by any contravention of the Data Protection Act.

9.2.6. To request the Information Commissioners Office (ICO) to assess whether any provision of the Act has been contravened.

9.3. Oasis Entities need to have in place effective means of extracting and retrieving information from a variety of sources in order to be able 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.

10. Lawful Processing and Consent

10.1. All Data Processing undertaken by Oasis must be lawful.

10.2. It is only lawful to undertake the Processing of PII on the following basis:

10.2.1. With the explicit consent of the data subject

10.2.2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

10.2.3. Processing is necessary for compliance with a legal obligation

10.2.4. Processing is necessary to protect the vital interests of a data subject or another person

10.2.5. 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

10.2.6. 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.

10.3. Where another basis for processing PII 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 as 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.

10.4. 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.

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

10.6. 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.

10.7. 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.

10.8. 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 that is 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.

10.9. Where consent has been obtained, it must be recorded. Oasis Entities are responsible for recording and maintaining an up to date record of the explicit consent that has been obtained where it is the basis of processing. Guidance on the recording of consent and example templates is available in the Oasis Guidance on Consent.

10.10. Consent can be withdrawn at any time. If consent it withdrawn, then any data held on the basis of the consent must be deleted/removed from Oasis Processing immediately.

11. Security of Electronic Data

11.1. 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, 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.

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

12. Security of Hard Copy (Paper Based) Data

12.1. The Oasis Information Security Policy sets out the requirements for the secure handling and management of Hard Copy Data 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.

12.2. Authorised individuals are individually responsible for the 'Hard Copy' PII in their care.

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

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

13. Retention and Disposal of Data

13.1. PII 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.

13.2. Hard Copy PII disposal must be through secure waste disposal. Guidance on the secure deletion/disposal of electronic information is available in the Oasis Information Security Policy.

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

14. Routine Publication of Information

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

14.1.1. Names of all Oasis Trustees including members of Oasis Committees including Committees, Boards and other current and future Governance forums.

14.1.2. Names, job titles and academic and/or professional qualifications of members of staff.

14.1.3. Awards and Honours including Prize winners.

14.1.4. Internal Telephone Directory.

14.1.5. Graduation programmes and videos or other multimedia versions of graduation, award and other ceremonies.

14.1.6. Information in prospectuses (including photographs), brochures, annual & other reports, staff newsletters, etc.

14.1.7. Staff information on Oasis website including photographs.

14.2. 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.

15. Communications and Marketing

15.1. 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 wider community.

15.2. 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.

15.3. 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.

16. CCTV

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

17. Disclosure of Personally Identifiable Information

17.1. Oasis will only disclose Personally Identifiable Information in its control in accordance with the Oasis Confidentiality Policy.

18. Safeguarding

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

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

19. Transfers of Data between Oasis Subsidiaries

19.1. Oasis entities that form part of the same legal subsidiary may share Personally Identifiable Information where required and in compliance with this and other Oasis policies.

19.2. 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.

19.3. Oasis UK will not transfer Personally Identifiable Information to another Oasis Subsidiary or Organisation outside of the UK for any purpose.

Appendix 1 – RACI Matrix

R : Responsible. A : Accountable. C : Consulted. I: Informed.

Policy Element			Leadership				Academy				Services													
	Board	Data Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of Strategic IT Projects	IT Technical Services Manager	Data Protection Officer	Service Desk Manager	National Service Desk	IT Service Manager	Cluster Manager	Onsite Teams	
1.3 Maintain OCL registration with ICO				A									I					R						
2.1-2.2 Data Classification (Academy)	I			I	I		A	R										C						
2.1-2.2 Data Classification (National Service)	I			I	I						A							C						
3.1 Overall accountability for Data Protection (DP) compliance	A		R	R	R	R	R	R		R	R		R	R	R	R	I	R						
3.3 Develop and maintain Policies, guidance, procedures to support Data Protection compliance			I	I	A		I						R	R	R			C	I	I	I			
3.4 Key point of contact for all data protection queries																		A						
3.5 Ensure that policies and processes are adhered to for Academy Data and by Academy Staff.	I			I	I	R	A	R		R								C						
3.6 Ensure that policies and processes are adhered to for nationally held data and by national staff within their service.	I			I	R			R			A	R						C						
3.8 Nominate DP leads (Academy)							A											I						
3.8 Nominate DP leads (National Service)											A							I						
3.12 Ensure any personal data they provide about themselves is up to date										A														
3.13 ensure third party agreed to comply with DP policy before they are granted access PII (Academy)	I			I	I	R	A	R					C	C				I	I	I	I	I	I	
3.13 ensure third party agreed to comply with DP policy before they are granted access PII (National Service)	I			I	R						A		C		C			C	I	I	I	I	I	

Policy Element			Leadership				Academy				Services													
	Board	Data Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of Strategic IT Projects	IT Technical Services Manager	Data Protection Officer	Service Desk Manager	National Service Desk	IT Service Manager	Cluster Manager	Onsite Teams
3.14 Maintain evidence that all those with access to PII have read and adhere to this policy. (Academy)	I			I		R	A	R										I					
3.14 Maintain evidence that all those with access to PII have read and adhere to this policy. (National Service)	I			I	R						A							I					
3.16 Complete DP training for new staff during induction and annually for all staff. Ensure evidence is recorded. (Academy)				I		R	A	R		R								I					
3.16 Complete DP training for new staff during induction and annually for all staff. Ensure evidence is recorded. (National Office)				I	R						A	R						I					
3.17 – 3.19 Additional in-person training for those with access to large volume or sensitive PII (Academy)				I		R	A	R										I					
3.17 – 3.19 Additional in-person training for those with access to large volume or sensitive PII (National Service)				I	R						A							I					
4.1, 4.3 Ensure each PII has owner (Academy)		I				R	A	R										I	I	I	I	I	I
4.1, 4.3 Ensure each PII has owner (National Service)		I			R						A							I	I	I	I	I	I
4.2, 4.5 Minimise processing of PII		A						R				R						C	I	I	I	I	I
4.6-4.7, 4.13 Catalogue PII (Academy)		R					A	R					I					R					
4.6-4.7, 4.13 Catalogue PII (National Service)		R									A	R	I					R					
4.9-4.10 Draft, publish and maintain privacy notice		C		A	R	R	R	R					R					C					
4.11 Develop, document and maintain policies and procedures for the safe and secure handling of PII (Academy)		C				R	A	R					C					C					
4.11 Develop, document and maintain policies and procedures for the safe and secure handling of PII (National Service)		C			R						A		C					C					
4.12➔4.14 Access to sensitive Data (Academy)		R				R	A	R					C					I	I	I	I	I	I
4.12➔4.14 Access to sensitive Data (National Service)		R			R						A		C					I	I	I	I	I	I

Policy Element			Leadership				Academy				Services													
	Board	Data Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of Strategic IT Projects	IT Technical Services Manager	Data Protection Officer	Service Desk Manager	National Service Desk	IT Service Manager	Cluster Manager	Onsite Teams
5.1-5.2 Conduct DP audits;	I		I	I	I		R	R			I		I					A					
5.3 Report to Board			I	I	I		I				I		I					A					
6.1-6.6 Conduct DP Impact Assessment (DPIA) (Academy)		R					A	R					C	C	C			C			C		
6.1-6.6 Conduct DP Impact Assessment (DPIA) (National Service)		R									A		C	C	C			C			C		
7.2-7.4 Report suspected DP breach		R		A	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R	R
8.1-8.6 Conduct DPIA on new systems and assess third parties as per Guidance. (Academy)		R				R	A	R			R		C	C	C			C			C		
8.1-8.6 Conduct DPIA on new systems and assess third parties as per Guidance. (National Service)		R				R					A		C	C	C			C			C		
9.3 Ensure process to retrieve information to comply with Subject Access Request (SAR) and other requests (Academy)		R				R	A	R			R		C	C				C			C		
9.3 Ensure process to retrieve information to comply with Subject Access Request (SAR) and other requests (National Service)		R			R						A		C	C				C			C		
10.1 – 10.10 Ensure that Processing is Lawful (Academy)						R	A	R										C					
10.1 – 10.10 Ensure that Processing is Lawful (National Service)					R						A							C					
11.1 – 11.4 Comply with Information Security policy & practices (Academy)		C				R	A	R		R			C	R	R			C	R	R	C	R	R
11.1 – 11.4 Comply with Information Security policy & practices (National Service)		C			R						A		C	R	R			C	R	R	C	R	R
12.2-12.6 Management of Hard Copy Data (Academy)		R				R	A	R	R									C					
12.2-12.6 Management of Hard Copy Data (National Service)		R			R						A							C					

Policy Element			Leadership				Academy				Services													
	Board	Data Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of Strategic IT Projects	IT Technical Services Manager	Data Protection Officer	Service Desk Manager	National Service Desk	IT Service Manager	Cluster Manager	Onsite Teams
13.1-13.3 Adherence to Data Retention Policy (Academy)		R				R	A	R	R									C						
13.1-13.3 Adherence to Data Retention Policy (National Service)		R			R						A							C						
14.2 Comply with valid request to opt-out of publication of information (Academy)		R				R	A	R		R	R	R						C						
14.2 Comply with valid request to opt-out of publication of information (National Service)		R			R		R	R		R	A	R						C						
15.1-15.3 Marketing: retain and maintain clear marketing lists with permissions; follow as per permissions (Academy)		R				R	A	R										C			C			
15.1-15.3 Marketing: retain and maintain clear marketing lists with permissions; follow as per permissions (National Service)		R									A							C			C			
16.1 Comply with CCTV policy (Academy)						R	A						C											
16.1 Comply with CCTV policy (National Office)					R						A		C											
17.1 Comply with Confidentiality policy when disclosing information (Academy)		R				R	A	R		R								C						
17.1 Comply with Confidentiality policy when disclosing information (National Service)		R			A						R							C						
18.1-18.2 Follow high level of care in processing safeguarding information by following all appropriate policies		R		R		R	A	R	R		R	R						C						
19.1➔19.3 Transfers of Data to Oasis Subsidiaries (Academy)	I	C		R		R	A	R					C					C	I	I	I	I	I	
19.1➔19.3 Transfers of Data to Oasis Subsidiaries (National Office)	I	C		R	R						A		C					C	I	I	I	I	I	

Appendix 2 – Systems & Business Process Ownership

System	Platform Management	Access Management	Data
Sims	IT Services	Academy	Academy
iTrent	People Directorate Payroll, Pensions and Compliance	People Directorate Payroll, Pensions and Compliance	People Directorate Payroll, Pensions and Compliance
PS Financials	IT Services	Finance Department	Finance Department
File Services (Academy)	IT Services	IT Services	Academy
File Services (National Service)	IT Services	IT Services	National Service

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 CEO, Dave Parr	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

Policy Tier

☒ Tier 1

☐ Tier 2

☐ Tier 3

☐ Tier 4

Owner

Director of Information Technology and Information Governance

Contact in case of query

sarah.otto@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
CSG	CSG	15-04-19	V1.31

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

Location

Tick all that apply:

☒ OCL website

☒ Academy website

☒ Policy portal

☐ Other: state

Customisation

☒ OCL policy

☐ OCL policy 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 Via Policy Portal	OCL	April 19	V1.31
DPL Group Via Email	DPLs	April 19	V1.31
OCL Via Bulletin	OCL	April 19	V1.31
OCL Via Policy Portal	OCL	Nov 19	V1.32