OASIS INFORMATION SECURITY POLICY

Dec 2017

Document Control

Changes History

Version	Date	Amended by	Recipients	Purpose
0.1-0.3	Dec 2017	Rob Lamont	Adam Turner, Shalin Chanchani	Drafts for discussion
1.0	Dec 2017	Rob Lamont	John Barneby, Dave Parr	Final Draft for approval

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version

Position with the Unions

Does the policy require consultation with the National Unions under our recognition agreement?
☐ Yes
☐ No

If yes, the policy status is:
☐ Consulted and Approved
☐ Consulted and Not Approved
☐ Awaiting Consultation

Distribution

This document has been distributed to:

Name	Position	Date	Version

CONTENTS

Purpose

The purpose of this document is to set out the Oasis policy on Information Security in a clear and transparent manner.

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 Oasis IT Services. Requests to change the policy should be made to the Head of Group IT Services. The policy has been developed in the context of the Oasis Ethos and Nine Habits of behaviour.

Policy Scope

This policy applies to both Electronic and Hard Copy data processed by Oasis.

The policy applies to all data processed by the following Oasis Entities:

- Oasis Community Learning
  - The Oasis Community Learning National Office
  - All Oasis Community Learning Academies
  - All Oasis Community Learning National Services
- Oasis Community Partnerships
  - The Oasis Community Partnerships National Office
  - All Oasis Community Partnerships Hub Charities
- The Oasis Charitable Trust
- The Oasis Foundation

Policy Principles

Oasis consider the security of Oasis data to be of the paramount importance and therefore the principle of this policy is that Oasis data will be protected wherever it is processed and it whatever form it is in. With this in mind, it is recognised that the needs of Oasis to access and process data always needs to be balanced against the importance of ensuring that the security of the data is not compromised.

Oasis recognises that different classifications of data have different levels of impact should it be accessed by those who do not have a need to do so. Therefore, different levels of security needs to be applied to different classifications of data. It is acknowledged that this may mean that the processing of sensitive data may be more difficult and time consuming that the processing of general data.

Policy Objectives

An objective of this policy is to ensure that Oasis data is always processed in a safe and secure manner such that it is not made available to those who are not authorised to have access to it and that it is available when required by those who do have legitimate need to access it.

An objective of the document is to set out the ways that Oasis data will be secured and managed by Oasis so that all staff and other users of Oasis services are clear on the requirements and responsibilities.

An objective of the policy is to provide transparency to Oasis data subjects around how data relating to them will be processed and to provide confidence that appropriate security measured will be applied.

Policy Strategy

The Oasis strategy for Information Security is to ensure that appropriate security measures are in place whether data is in use, at rest or in transit. The use of physical, technical, organisational process and policy controls provide these security measures. The strategy is to provide multi-level security around Oasis data to mean that if for whatever reason a particular control fails, then another will prevent the unauthorised access to data.

Related Oasis Policies, Standards and Processes

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

- The Oasis Data Protection Policy
- The Oasis Acceptable Use of Technologies Policy
- The Oasis IT Security Policy
- The Oasis Web Filtering Policy
- The Oasis IT Asset Management Policy
- The Oasis Backup and Retention policy
- The Oasis IT Access Policy
- The Oasis IT Change Management Policy

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

- The Oasis IT Services Web Filtering Configuration Standard
- The Oasis IT Services Internet Access Monitoring Standard
- The Oasis IT Services Resource Access Standard
- The Oasis IT Services Standard for Guest Access to the IT System
- The Oasis IT Services IT Physical Infrastructure Security Standard
- The Oasis Standard for Hard Copy Data Physical Security.

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

- The Oasis Assessment of Third Party Data Processors Process
- The Oasis User Creation Process
- The Oasis User Deletion Process
- The Oasis IT Business Continuity Process

Applicable Legislation, Guidance and References

- Data Protection Act 1998
- General Data Protection Regulation.

Definitions

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

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 Processing: See Processing

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.

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.

OCMS: The Oasis Call Management System, used by Oasis IT Services and by system users to record incidents, requests, changes and problems within the operation of the IT System to be resolved. Calls or tickets recorded in this system provide the identifier and audit trail of actions carried out by the Oasis IT Services team on the Oasis IT System and form the basis for recording authorisation for these works to be undertaken.

Personal Data; Otherwise known as Personally Identifiable Information. 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 should be considered as Personal Data.

Personally Identifiable Information (PII): See Personal Data and Sensitive Data. Personally, Identifiable information is the collective term used for information relating to an individual that in Oasis has been classified as Sensitive or Personal.

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: Different from ordinary PII (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

User Account: The most import component of a user's ability to gain access to an Oasis IT Services Managed Resource is the 'User account'. The user account is the basic identifier through which access is allowed or denied. User account are associated with a named person. The association may in the form of the account being assigned to an individual member of Oasis or it may be sponsored by an Oasis staff member who is accountable for its use but assigned to an individual who is not an Oasis employee or staff member.

Users: Users are individuals who make use of the Oasis IT Services IT System. They include students, staff, contractors, consultants, temporary employees, volunteers, business partners, guests and visitors.

Policy Statements

1. Technical Security Considerations

1.1. Oasis will manage Oasis IT Systems in accordance with the Oasis IT Security Policy.

1.2. Access to the Internet from within the Oasis IT System is monitored and filtered. This monitoring and filtering will be conducted as set out in the Oasis Web Filtering policy.

1.3. Oasis IT Services will implement policies which impose security policies on mobile devices to meet the requirements of this policy. This will include the use of Oasis IT managed services on Personally Owned Devices. These security policies will include the ability to remote wipe a device without notice.

Encryption

1.4. The minimum encryption standard used to secure Oasis data will be AES-256bit unless specifically authorised by the Head of IT Services and the Data Protection Officer.

1.5. All Oasis client devices primary used by Oasis Staff and all client devices used for the storage of Personally Identifiable information must have full drive disk Encryption enabled to a minimum of AES-256bit.

1.6. All Oasis Servers will have full drive disk Encryption enabled to a minimum of AES-256bit.

1.7. Oasis Services published over the internet will be published via HTTPS and will be protected to a minimum of SHA256 security standard.

Backup

1.8. All Oasis Servers and the data stored on them will be protected via a backup regime detailed in the Oasis Backup and Retention policy.

1.9. Oasis Client Devices are not backed up by Oasis IT Services and therefore the use of local storage on Client Devices is not recommended.

Control of Access

1.10. All systems and devices that provide access to Oasis data must be accessed by means of an authenticated user account.

1.11. Management of Access to Oasis IT Services Managed IT Services will be undertaken as per the Oasis IT Access Policy and changes will be authorised as per the Oasis IT Change Management Policy and Process.

1.12. All Oasis IT Services solutions used to access Personal or Sensitive data must be authenticated as part of the Oasis IT Services Active Directory Domain.

Use of Public Wi-Fi

1.13. Use of public Wi-Fi or third party managed Wi-Fi solutions can present a security risk as it is possible that the use of the system may include interception of data that is transmitted via the wireless system. The installation of third party certificates is sometimes required for the use of these solutions which in turn may facilitate the interception of the content of secure web pages and emails.

1.14. Users making use of public Wi-Fi solution must ensure they are aware of the security implications around the use of public Wi-Fi and ensure that it is only used where unauthorised access to Oasis data is not facilitated.

1.15. Users must not use public Wi-Fi for the access to or transmission of Oasis Confidential or Personally Identifiable Information.

2. Electronic Data

Physical Security of Oasis Electronic Data

2.1. Oasis IT infrastructure must be deployed to the Oasis IT Services IT Physical Infrastructure Security Standard

2.2. The use of Oasis IT equipment must be conducted in accordance with The Oasis Acceptable use of Technologies Policy.

2.3. Oasis IT equipment should remain within Oasis premises unless it has been specifically authorised for use away from an Oasis location.

2.4. Only Oasis IT Client devices configured for staff use may be authorised for use by Oasis staff away from Oasis premises.

2.5. Devices used away from Oasis premises must be issued to an individual staff member who is responsible for ensuring that the device is protected in accordance with the Oasis Asset Management Policy.

At Rest - General Electronic Data

2.6. All data processed during the course of undertaking duties for or on behalf of Oasis is considered to be Oasis Data.

2.7. Oasis provides a range of systems for the storage of electronic data. Oasis Data should only be stored within these systems or within authorised third party platforms where they have been approved for use as per the Oasis Assessment of Third Party Data Processors Process.

2.8. Permitted storage locations for Oasis Data within the Oasis IT system are:

- Home Drives within the Oasis Network
- Shared Drives within the Oasis Network
- Oasis provided OneDrive for Business
- Oasis provided SharePoint Document Libraries (the OasisZone)
- Within Oasis hosted applications including email and databases
- Within third party hosted applications and databases where the third party has been approved as an Oasis Data Processor.

2.9. A list of approved third party storage locations that have been approved under the Oasis Assessment of Third Party Data Processors Process is available from the Oasis IT Service Desk.

2.10. The use of local storage on Oasis devices which meet the other requirements of this policy is not recommended but is permitted. However, data stored in these locations is not protected by a backup provided by Oasis IT Services and therefore user does so at their own risk. The user is responsible for ensuring that the data is appropriately backed up to another permitted storage location.

2.11. Devices that are returned to Oasis IT Services for maintenance or repair may be wiped without notice. It is the user's responsibility to ensure that all data is backed up prior to returning the device to Oasis IT Services.

2.12. The failure to appropriately protect and ensure the availability of data which a user is responsible for, resulting in its loss may be considered a disciplinary offence up to and including gross misconduct.

2.13. Synchronisation of Oasis Data onto personally owned devices is permitted where;

- The primary storage location of the data remains one of the locations above and the data is synchronised to other locations; for example, it is permitted to synchronise email onto a personally owned mobile phone.
- **And**; the device in question is being used in accordance with the Use of Personally Owned Devices (UPOD) policy.

At Rest – Confidential Data

2.14. Confidential Data requires additional precautions to be taken for its processing and has requirements that exceed those for General Oasis Data. All of the provisions of this policy required for the storage of General Oasis Data apply to the storage of Confidential Data unless detailed following:

2.14.1. All Confidential Data must be protected at a file level or stored in an approved secure storage platform. File level protection means that the file itself will be protect through encryption rather than being only protected by the encryption of the disk. The Oasis approved method for undertaking this on the Oasis IT System is via Microsoft Office 365 Rights Management Services (RMS). Guidance of the use of RMS can be found in the Oasis Guidance on RMS File Protection Document.

2.14.2. Confidential Data should not be stored on Personally Owned Devices except where it is contained within email or has been received via email and the email synchronised onto the device. In these circumstances, the user should take steps to move the information to an appropriate alterative system and ensure that the content is removed from email as soon as possible.

At Rest – Personal Data

2.15. Personal Data requires additional precautions to be taken for its processing and has requirements that exceed those for general Oasis Data. All of the provisions of this policy required for the storage of General Oasis Data apply to the storage of Personal Data unless detailed following:

2.15.1. Personal Data should not be stored on local device storage except where it is contained within email or where is synchronised with another Oasis IT System location.

2.16. The storage of Personal Data on Personally Owned Devices is only permitted where the Personally Owned Device has been configured as the per security requirements set out for Oasis Owned Client Devices in this policy with the exception of user authentication as detailed in 1.11.

At Rest - Sensitive Data

2.17. Sensitive Data requires additional precautions to be taken for its processing and has requirements that exceed those for General Oasis Data and for Personal Data. All of the provisions of this policy required for the storage of general Oasis Data and Personal Data apply to the storage of Sensitive Data unless detailed following:

2.17.1. All Sensitive Data must be protected at a file level or stored in an approved secure storage platform such as CPOMS. File level protection means that the file itself will be protect through encryption rather than being only protected by the encryption of the disk. The Oasis approved method for undertaking this on the Oasis IT System is via Microsoft Office 365 Rights Management Services (RMS). Guidance of the use of RMS can be found in the Oasis Guidance on RMS File Protection Document.

2.17.2. Sensitive Data should not be stored on Personally Owned Devices except where it is contained within email or has been received via email and the email synchronised onto the device. In these circumstances, the user should take steps to move the information to an appropriate alterative system and ensure that the content is removed from email as soon as possible.

2.17.3. Sensitive Data must be held exclusively within Oasis Systems or approved storage platforms. This includes the implementation of synchronisation to Personally Owned Devices where selective sync must be used to ensure that Sensitive Data is not synced to the device.

At Rest - Use of Physical Storage Media

2.18. Physical Media is considered to be the use of any USB Storage Device such as an external flash drive, any magnetic media such as a backup tape or Optical Media such as a CD, DVD or BluRay.

2.19. Physical media may be used in some circumstances to facilitate the transit of data between systems where no alternative solution is available and where it meets the requirements for data in transit set out later in this document.

2.20. The use of Physical Storage media is not permitted for the storage of Oasis Data with the exception of the use by the Oasis IT Services team under specific circumstances detailed later.

2.21. The Oasis IT Services team are permitted to make use of Physical Storage media course of their duties where:

- The storage is only temporary and being used as a means of transferring data between systems and Full Disk Encryption to a minimum of AES-256bit standard has been applied to the portable storage media before the data transfer to it has taken place.
- The storage is being used for the introduction of software tools to other devices for example containing original media being used to install software
- The storage is being used to provide ‘boot services’ for other client devices.
- The use of Optical or Magnetic Media for the creation and maintenance of backups
- Other circumstances specifically authorised by Head of IT Services

In Use - Electronic Data

2.22. Users should always give consideration to whether other individuals can see display screens when data is in use. Personal and/or sensitive data should not be processed when display screens are over looked or can be viewed by those who are not authorised to access the data.

2.23. When processing personal or sensitive data users should be conscious of the movement of people around them. Users should minimise or close electronic data files when someone moves into a position where they may be able to view the data

2.24. Monitors should be positioned to limit the positions from where the screens can be viewed including through windows if they are to be used for the processing of Personal and Sensitive Data to limit the risk of casual observation of the data.

2.25. Where devices are regularly used for the processing of personal or sensitive data then screen protection should be introduced.

2.26. The regular processing of sensitive data should be undertaken in areas where physical access is restricted.

2.27. Users should ensure that devices are locked if they step away from the device at any point.

In Transit – General Data

2.28. Data in transit is at significant risk of loss or interception if appropriate security precautions are not taken.

2.29. The risks associated with the transfer should be considered and where large amounts or sensitive data are involved then a specific risk assessment should be undertaken with appropriate mitigations considered before the transit is authorised. The risk assessment should be stored in an OCMS call along with the authorisation for the transfer.

In Transit - Transfer Third Parties

2.30. The Oasis Confidentiality Policy outlines the circumstances where data can be transferred from Oasis to a third party. This policy outlines the security precautions and pre-requisites should the transfer be deemed to be required and authorised under the Oasis Confidentiality Policy.

2.31. The level of precautions that are required will depend on the sensitivity level of the data being transferred and the type of data being protected.

2.32. All data being provided to a third party should be encrypted at a file level. Guidance on Encrypting Oasis Data Files for Transfer to third parties can be found in the Oasis IT Service Guidance in the use of file encryption document.

2.33. If physical media is used then encryption should also be implemented on the media as well as at a file level.

In Transit – Use of Physical Media

2.34. Physical Media is considered to be the use of any USB Storage Device such as an external flash drive, any magnetic media such as a backup tape or Optical Media such as a CD, DVD or Blu-Ray.

2.35. The use of Physical Media to move data between locations is considered to be a high-risk scenario and should be avoided if at all possible. Movement of data via Physical Media should only be undertaken when no alternative mechanism is available and the transfer is required.

2.36. The transit of data between home and work is not a scenario where the use of Physical Media would be permitted.

2.37. The transport of data using physical media must be specifically authorised in advance of the transport taking place by the Data Protection Lead for the Oasis entity. The authorisation must be recorded through the OCMS system.

2.38. All Oasis Data Transferred via Physical Media must be authorised as 'in and out' of the Oasis Entity by the person responsible for the transfer in the OCMS system and counter authorised by the Data Protection Lead.

2.39. Physical Media must be encrypted to the AES-256bit standard via the Physical Media. If the data is sensitive then it must be protected both on the physical media and at a file level using an approved encryption method.

2.40. The physical media must be wiped or destroyed using an approved data destruction method once the transfer of the media is complete.

Ensuring the availability of Oasis Electronic Data

2.41. All Oasis data must be protected to ensure that it is available whenever it is required.

2.42. Data will be protected as per the Oasis Backup and Retention Policy.

2.43. Access to the Data will be ensured through the implementation of the Oasis IT Services Business Continuity Process.

Destruction of Electronic Data

2.44. 'Deletion' of data from electronic media does not ensure that it is permanently destroyed.

2.45. In order to ensure that electronic data has permanently been destroyed then the media holding the data must either be physically destroyed or sanitised using a software solution certified by the National Cyber Security Centre[1].

[1] https://www.ncsc.gov.uk/index/certified-product?f%5B0%5D=field_assurance_status%3AAssured&f%5B1%5D=field_product_type%3A68

3. Hard Copy Data

At Rest - Hard Copy Data

3.1. Hard Copies of Oasis Data must be protected by appropriate physical security for its classification. This includes when data is offsite. Where there is a need for Hard Copy PII to be taken Off-site such as to a staff members home addresses, restricted access to the data should be maintained and appropriate precautions must be taken to prevent others including family members from gaining access to the information.

3.2. All paper files and documents containing Personal Sensitive or confidential data must be kept in secure, lockable cabinets. These cabinets must be kept locked, and the keys in secure locations. Cabinets must not be left unlocked for convenience. The location of keys must be kept confidential and not be easily accessible to non-authorised persons.

In Use - Hard Copy Data

3.3. Users must always give consideration to the security of Hard Copy Data from the point of production. When files or any records are printed, users must ensure that they cannot be accessed or viewed by individuals who are not authorised to access the data.

3.4. Personal and/or sensitive data must not be left unsupervised when not in use. It must be stored securely as per the provisions outlined later in this document.

3.5. Users must ensure that when working with personal/sensitive hard copy data they are aware of other individuals around them and take appropriate steps to ensure that it cannot be viewed by those not authorised to do so. This may involve turning documents over or covering documents when other individuals move into positions where the documents can be viewed.

3.6. The regular processing of sensitive data should be undertaken in areas where physical access is restricted.

In Transit - Hard Copy Data

3.7. In general, there is a presumption against taking personal or other confidential data contained within paper records off-site.

3.8. Material should only be taken off-site when it is a necessity and not just a convenience. Users must consider how much information is actually required and take off-site only what is really required.

3.9. Where data contained within paper records is taken off-site it should be kept to a minimum in terms of content and duration.

3.10. The transfer of personal or sensitive hard copy data outside of Oasis premises must be specifically authorised by the Data Protection Lead. Consideration must be given to requirement for the transfer and the business need balanced against the risks of the transit before authorisation is granted. Authorisation for the transit for significant amounts of Personal Data or for Sensitive Data should only be granted following completion of a Data Protection Impact Assessment (DPIA) and Risk Assessment (RA). The DPIA and RA must be retained and records of the data being processed and the authorisation retained by the Oasis Entity

3.11. The loss of a large amount of Hard Copy data in transit could have a significant impact on both the data subjects effected and the on Oasis. Therefore, the transit of large amounts of hard copy data together must be minimised.

3.12. Where large amounts of hard copy data are required to be transported then consideration must be given to the transit being undertaken in electronic format. Electronic records of Sensitive, Personal and Confidential Data should be stored in a secure separate location. Hard copy transit of data should only be undertaken when after due consideration it is concluded that the use of hard copy data is required.

In Transit - Hard Copy Data by Oasis Staff

3.13. Oasis Staff may need to physically transfer hard copy data between locations.

3.14. Where Sensitive, Confidential or Personal Data is being transferred then it must be kept in the staff members possession at all times and must not be left unsupervised in vehicles or other vulnerable locations.

3.15. In the event that a user suffers a loss of Hard Copy Data, they will need to be able to satisfactorily demonstrate that they have followed appropriate procedures and taken due care. Some measures users can undertake include the following:

3.15.1. Do not carry 'loose' paper records as this increases the risk of dropping or losing them, make sure documents you carry are safe within a folder or other appropriate container.

3.15.2. Do not carry paper records in a bag containing valuables, as these are often the primary target for thieves.

3.15.3. Ensure paper records are not in transit for any longer than is necessary, and they are delivered to their destination at the earliest opportunity.

3.15.4. Do not leave bags or cases containing paper records visible in a car; if it is unavoidable to store paper records in a car, lock them in the boot. Do not leave paper records stored in the boot of an unattended vehicle.

3.15.5. When travelling on public transport ensure that the contents of paper records are not visible.

3.15.6. When travelling on public transport keep bag/case containing paper records close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of loss or theft.

3.15.7. Treat paper records as you would your cash. In case of loss of Personal, Confidential or Sensitive data, notify your Data Protection Lead immediately.

3.15.8. Ensure confidential paper waste created away from the office environment is securely disposed of using a cross cut shredder or ensure this is safely returned to Oasis premises for secure destruction.

In Transit – Use of Postal/Shipping Services with Hard Copy Data

3.16. The use of postal or courier services is considered to be a secure method of transit for the actual movement of the Hard Copy Data. However, there are significant risks associated with it use such as ensuring that the data is not lost in transit, is received by the correct person and is both sent and delivered to the correct address of the intended recipient. As such the use of the postal or courier services must be undertaken with caution.

3.17. The recipient address for the sending of personal and/or sensitive data must be positively confirmed before it is sent.

3.18. Where personal and/or sensitive data is sent then it must be sent via a service where its location can be tracked and a signature is required to acknowledge receipt of the information.

3.19. When sending sensitive data, the sender must notify the recipient of the intending shipping of the information including the expected delivery window.

3.20. The sender must positively confirm that the hard copy data has been received.

3.21. The sender must ensure that the data is appropriately packaged so the contents are not visible other than when the documents are opened. For the sending of Personal and/or Sensitive data then secure, tamper proof packaging should be used.

3.22. Personal data sent via the postal or courier service should be clearly addressed to a known individual and secured in a sealed envelope marked “Private and Confidential”.

3.23. For sensitive data, an inner and outer envelope must be used. The inner envelope must be Securely sealed and clearly addressed to a known contact and marked “Private and Confidential - To be opened by the addressee only”. The second outer envelope should be clearly addressed to the known contact.

3.24. The sender address should be added to the back of the package for Confidential, Personal and/or Sensitive data so that the information can be returned should a delivery not be successful.

Destruction of Hard Copy Data

3.25. All Oasis Entities must develop and adhere to a process for the secure destruction of data that is approved by the Data Protection Officer.

4. Email

Use of Email

4.1. Oasis provides an email system for the purposes of conducting Oasis business. Users must conduct email communications around Oasis business exclusively using the provided Oasis email account. The use of personal email accounts or email services hosted by third parties by Oasis staff for the processing of Oasis data is expressly prohibited by this policy. This includes both the sending and receiving of email through a third-party service.

4.2. The use of the POP3 email protocol is not permitted and will be disabled by Oasis IT Services.

4.3. The SMTP email protocol must only be used in conjunction with SSL to ensure that the communication is encrypted.

4.4. Users must ensure that care is taken to verify that the recipient email address used is that of the intended recipient. This includes the use of distribution lists within the Oasis IT System.

4.5. Oasis maintains a directory of Oasis email addresses as part of the email system. This list is automatically updated by Oasis IT Services as part of the Oasis User Creation Process and Oasis User Deletion Process.

Transmission of Data via Email

4.6. Email is not a secure mechanism for transferring data. It is both prone to accidental transmission of data to unintended recipients and open to interception in transit. It should not be used for the transmission of Oasis Data unless appropriate precautions are taken.

Forwarding of Email

4.7. Forwarding of email is considered to be where a single or group of emails is manually forwarded from the addressee to another email address. Emails are sent to specific addressees and may contain confidential, personal and sensitive data. Any forwarding of emails should only be carried out in accordance with the Oasis Confidentiality Policy.

4.8. Auto forwarding is where technology is used to automatically forward email to another email address. Auto forwarding rules will not be placed on 'named' Oasis User Accounts. This includes forwarding implemented by the Services Team IT or by the user themselves for any purpose.

4.9. Oasis IT Services will block the creation of forwarding rules through Microsoft Office 365 Outlook Web Access.

4.10. Oasis IT Services will monitor the use of forwarding rules and will remove email forwarders implemented without notice where they are detected.

4.11. Auto forwarding can be used from a generic unnamed mailbox such as one representing a function or service. Where multiple users need access to incoming mail to a generic unnamed email address then a shared mailbox should be used except where replies from the generic mailbox are not necessary.

Interception and Mirroring of Email

4.12. Email Interception is considered to be where incoming email to the Oasis IT System from a particular email address or addresses is automatically sent to another mailbox. This is distinct from email auto forwarding where email to a particular address would be forwarded. Oasis will not implement email Interception within the Oasis IT System.

4.13. Email Mirroring is considered to be where all email sent from a particular Oasis email account is automatically forwarded to another mailbox. Oasis will not implement email Mirroring within the Oasis IT System.

Distribution Lists

4.14. All distribution lists configured within the Oasis IT Services IT system must have security applied to them to limit who can send to the addresses.

4.15. Distribution Lists should be considered a shared resource under the Oasis IT Access Policy and the ability to send to the distribution lists should be managed in accordance with that policy.

5. Third Party Repair of Oasis Client Devices

5.1. From time to time, it may be necessary for Oasis Client Devices to be given to a third party for the purposes of maintenance or repair. In such circumstances, the security of any Oasis Data stored on the device is paramount.

5.2. Where possible, in the first instance the internal storage should be securely wiped before the device leaves Oasis supervision in accordance with the Guidance of the Destruction of Data. Depending on the nature of the fault it is recognised that this may not be possible.

5.3. Where this is not possible then the internal storage should be removed from the device before it leaves Oasis supervision. Again, it is recognised that this may not be always possible for technical reasons.

5.4. If the device only contains Oasis General Data and the device is encrypted to the AES-256bit standard, then the device can be sent for repair as long as the password to unlock the disk encryption is not supplied.

5.5. If the device contains Personally Identifiable Information and/or Sensitive Data and one of the previous steps outlined is not possible, then the device cannot leave Oasis supervision for the repair. If a repair can be undertaken under Oasis supervision then the repair can proceed. If this is not possible then the repair must not be undertaken and the device may need to be written off.

Appendix 1 – RACI Matrix

Policy Element		Leadership				Academy				Services		IT Team										
	Policy Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	National Service User	Head of IT Services	National Service Delivery Manager	National Infrastructure Manager	National Programme Manager	National IT Operations Manager	Data Protection Officer	Service Desk Manager	National Service Desk	Regional Service Delivery Manager	Cluster Manager	Onsite Teams
1.1 Management of IT in accordance with the IT Security Policy		I	I	I		I			I	I	I	A	R	R	R		C	R	R	R	R	R
1.2 Management Internet Access in accordance with Web Filtering Policy				I	I	I			I	I	I	A	R	R				R	R	R	R	R
1.3 Imposition of Mobile Device Security				C	I	I			I	I	I	A	C	R	I		C	I	I	I	I	I
1.5 Encryption of Oasis Staff Devices				C	I	I			I	I	I	A	R	R	R		C	R	R	I	R	R
1.6 Encryption of Oasis Servers				C	I	I			I	I	I	A	I	R	R		C	R	R	I	R	I
1.8 Implementation Backup as Per the Backup & Retention Policy												A	C	R			C	R	R	I	R	I
1.10 ➔ 1.12 Control of Access												A	R	R			C	R	R	R	R	R
1.14 ➔ 1.15 Use of Public Wi-Fi (Academy)						R			A								C					
1.14 ➔ 1.15 Use of Public Wi-Fi (National Service)										R	A						C					
2.1 Implementation of IT Physical Security Standards						R				R		A	R	R	R		C	R	R	R	R	R
2.2 ➔ 2.5 Use of Client Devices (Academy)						R			A			I	C							R	R	R
2.2 ➔ 2.5 Use of Client Devices (National Service)										R	A	I	C							R	R	R
2.7 ➔ 2.13 Correct Storage General Data at Rest (Academy)						A	R	R	R			C	C	R			C			C	R	I
2.7 ➔ 2.13 Correct Storage General Data at Rest (National Service)										A	R	C	C	R			C			C	R	I
2.14 Correct Storage Confidential Data at Rest (Academy)						A	R	R	R			C	C	R			C			C	R	I
2.14 Correct Storage Confidential Data at Rest (National Service)										A	R	C	C	R			C			C	R	I
2.15 ➔ 2.16 Correct Storage Personal Data at Rest (Academy)						A	R	R	R			C	C	R			C			C	R	I
2.15 ➔ 2.16 Correct Storage Personal Data at Rest (National Service)										A	R	C	C	R			C			C	R	I
2.17 Correct Storage Sensitive Data at Rest (Academy)						A	R	R	R			C	C	R			C			C	R	I

2.17 Correct Storage Sensitive Data at Rest (National Service)										A	R	C	C	R			C			C	R	I
2.20 Use of Physical Media for Storage of Data (Academy)						A	R		R			C	C	R			C			C	R	I
2.20 Use of Physical Media for Storage of Data (National Service)										A	R	C	C	R			C			C	R	I
2.21 IT Services User of Physical Media												A	R	R	R	R		R	R	R	R	R
2.22➔2.27 Visibility of display screens (Academy)										A	R									C	C	C
2.22➔2.27 Visibility of display screens (National Service)						A	R		R											C	C	C
2.28 ➔ 2.29 Electronic Transit of Data (Academy)						A	R		R			C	C	R			C			C	R	I
2.28 ➔ 2.29 Electronic Transit of Data (National Service)										A	R	C	C	R			C			C	R	I
2.30 ➔ 2.33 Transfer of Data to Third Parties (Academy)						A	R		R			C	C	R			C			C	R	I
2.30 ➔ 2.33 Transfer of Data to Third Parties (National Service)										A	R	C	C	R			C			C	R	I
2.34 ➔2.40 Transfer of Data using physical Media (Academy)						A	R		R			C	C	R			C			C	R	I
2.34 ➔2.40 Transfer of Data using physical Media (National Service)										A	R	C	C	R			C			C	R	I
2.41 ➔ 2.43 Ensuring the Availability of Oasis Data												A		R			C	R	R	R	R	R
2.44 ➔ 2.45 Secure deletion of data												A		R			C	R	R	R	R	R
3.1 ➔ 3.2 Storage of Hard Copy Data (Academy)						A	R		R								C					
3.1 ➔ 3.2 Storage of Hard Copy Data (National Service)										A	R						C					
3.3 ➔ 3.6 Use of Hard Copy Data (Academy)						A	R		R								C					
3.3 ➔ 3.6 Use of Hard Copy Data (National Service)										A	R						C					
3.7 ➔ 3.12 Hard Copy Data Offsite (Academy)						A	R		R								C					
3.7 ➔ 3.12 Hard Copy Data Offsite (National Service)										A	R						C					
3.13 ➔ 3.15 Transfer of Hard Copy Data by Staff (Academy)						A	R		R								C					
3.13 ➔ 3.15 Transfer of Hard Copy Data by Staff (National Service)										A	R						C					
3.16 ➔ 3.24 Use of Postal / Courier Services (Academy)						A	R		R								C					
3.16 ➔ 3.24 Use of Postal / Courier Services (National Service)										A	R						C					
3.25 Hard Copy Data Destruction Process (Academy)						A	R		R								C					
3.25 Hard Copy Data Destruction Process (National Service)										A	R						C					
4.1 Use of third party email services (Academy)						R			A													
4.1 Use of third party email services (National Service)										R	A											
4.2➔4.5 Management of the Email Service												A	I	R				R	R	I	R	R
4.6 Transmission of data via email (Academy)						A	R		R								C				C	C

4.6 Transmission of data via email (National Service)										A	R						C				C	C
4.7 Forwarding of email (Academy)						A	R		R											C	C	C
4.7 Forwarding of email (National Service)										A	R									C	C	C
4.8 ➔4.11 Monitoring of Auto forwarding Rules												A		R				R	R			
4.12 Email Interception			A									R		R								
4.13 Email Mirroring			A									R		R								
4.14 Security on to distribution lists												A		R				R	R		R	R
4.15 Management of Access to distribution lists												A	R	R				R	R		R	R
5 Third Party Repair of Oasis Client Devices												A	R				C	R	R	R	R	R