IT SECURITY POLICY

April 2021

CONTENTS

1. Introduction and the Oasis Vision, Ethos and 9 Habits

1.1 The purpose of this policy is to set out the approach to IT Security adopted by Oasis.

1.2 In setting a policy for IT Security, the Oasis vision is important. Our vision is for community – a place where everyone is included, making a contribution and reaching their God-given potential. Our ethos is a statement of who we are and it is an expression of our character. Rooted in the story and beliefs of Oasis, we describe our ethos through a particular set of values that inform and provide the lens on everything we do.

- **A passion to include**
- **A desire to treat people equally respecting differences**
- **A commitment to healthy, open relationships**
- **A deep sense of hope that things can change and be transformed**
- **A sense of perseverance to keep going for the long haul**

1.3 It is these ethos values that we want to be known for and live by. It is these ethos values that also shape our policies. They are the organisational values we aspire to. We are committed to a model of inclusion, equality, healthy relationships, hope, and perseverance throughout all the aspects of the life and culture of every Oasis Hub and community.

1.4 Everyone who is part of Oasis needs to align themselves to these ethos values. The values themselves are inspired by the life, message and example of Jesus but we make it clear that we will not impose the beliefs that underpin our ethos values. We recognise and celebrate the richness that spiritual and cultural diversity brings to our communities. We respect the beliefs and practices of other faiths and will provide a welcoming environment for people of all faiths and those with none.

1.5 Therefore, right at the heart of Oasis is this deep-rooted commitment to inclusion, equality, good relationships, hope and perseverance. This is inescapable and must be core to our delivery of this IT Security policy. We are committed to providing a safe environment for all our staff and our students so they can work and learn in a relaxed, secure atmosphere and have every opportunity to thrive and become the very best version of themselves. Every single one of us has a part to play in making this possible and this is laid out clearly throughout this policy.

The Oasis 9 Habits

1.6 The Oasis ethos is aspirational and inspirational and something that we have to constantly work at. It is important to remember that every organisation is made up of its people, and people don't always get things right every day. This means that there can sometimes be a dissonance between what we say we are, as stated in our ethos values, and what we actually do and experience. Recognising this is helpful because it reminds us that we each have things to work on; we have space to grow, develop and change to become the best version of ourselves. The 9 Habits our bespoke and unique approach to character development.

1.7 We know that by living the way of the habits, the Oasis ethos behaviours we aspire to will become second nature to us. This is vitally important for all staff to understand and engage in for the carrying out of this IT Security policy in Oasis. The 9 Habits are also core to all of our

students as they learn how to behave online and be committed to the development of healthy positive life-bringing relationships that enable them and others to flourish.

1.8 Everything within this policy has been developed in the context of and through the lens of the Oasis Ethos and 9 Habits.

All of this is detailed in our Education Charter.

Introduction

1.9 Oasis operates an extensive IT Infrastructure to facilitate and enable the work of various parts of the Oasis family in supporting the development of community. The IT infrastructure is both the container for large amounts of data which needs to be protected and a vital utility on which the Oasis family depends for its day-to-day operation.

1.10 The loss of personal data can have profound consequences for the individuals that we serve. Oasis have a moral and legal responsibility to do everything that we can to ensure that this information is effectively protected at all times. This is a clear commitment to our ethos values.

1.11 Unauthorised access to organisational data and systems could cause embarrassment to Oasis but also could allow confidential and critical information to be used to defraud the Oasis family of funds that should be used to support our work.

1.12 Disruption to IT services including the prevention of access to system resources impacts the work that we do and prevents us from achieving our objectives.

1.13 We operate in a world of increasing IT cyber security threats with individuals and organised criminals seeking to breach IT system defences for a variety of reasons. As the use of technology continues to expand the exposure to these risks increases.

1.14 The security of the IT systems is designed to minimise the risk of Oasis being damaged by the consequences of these threats from being realised. This policy is designed to outline both the approach and the specific requirements for IT Security for these risks to be effectively managed.

1.15 Many of the requirements outlined in this policy are the responsibility of those with specific involvement with the management of the IT system and its implementation. However, there is a broader responsibility for all members of the Oasis family to ensure that their seemingly small individual actions and decisions do not provide avenues for the IT Security of the family to be compromised. Whilst IT Security can sometimes seem restrictive, preventing the continuation of other important work, effective IT Security is essential to ensure that Oasis can effectively continue our work.

1.16 This policy is maintained by Oasis IT Services. From time to time, we may amend this policy. Requests to change the policy should be made to the Director of Information Technology.

2. What is this policy about?

In brief

2.1 This policy sets out the requirements, responsibilities and accountabilities associated with this policy including both a high-level overview of the technical controls in place and the actions and behaviours that must be adhered to by users. 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.

In more detail

Policy Principles

2.3 Oasis seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting users in working towards Oasis objectives. This also requires the integrity and confidentiality of the Information Technology Infrastructure and systems to be maintained. It is a principle of this policy that the requirements of the organisation to change and develop rapidly, the need to be flexible in our use of Technology and to be entrepreneurial in the approach to problem solving are balanced against the IT Security Risk faced.

2.4 A principle of this policy is to meet, in all regards, the requirements of the UK Government's Cyber Essentials Security Standard and where appropriate to provide a higher degree of security where there is a particular requirement to do so. At all times, this policy seeks to follow National Cyber Security Centre (NCSC) best practice guidelines.

Policy Strategy

2.5 A key strategy of this policy is to implement the technical requirements of the UK Government's Cyber Security Essentials Standard across the estate, to ensure that certification can be maintained.

2.6 Where the requirements of the standard do not apply or are not defined then the strategy of the policy is to adopt a risk-based approach which balances the risk presented from a particular threat against the need for the organisation to be able to make effective use of technology.

Policy Objectives

The objectives of this policy are to:

- Ensure the security and integrity of the Oasis IT infrastructure by setting out how we will effectively mitigate the risk of unauthorised access, damage to or theft from the Oasis IT estate.
- Provide clear and detailed technology and infrastructure configuration and deployment requirements which can be used to evaluate the security of new solutions proposed and developed for use within the Oasis IT estate.
- Ensure that staff and students are protected from potential risk in their use of IT in their everyday work including the inadvertent actions which could lead to significant disruption to services.

Definitions

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

Future Cloud: See PCE below.

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.

PCE/Policy Central Enterprise/SMM/Smoothwall Moderated Monitor: A system used to record safeguarding related activity on a client device

RADAR: See PCE

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.

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.

Web Filtering: Is the restriction and prevention of access to individual and groups of websites based on the content. Oasis IT Services currently deploy a solution from the manufacturer Smoothwall to implement Web Filtering across the Oasis IT Services network.

3. Who is this policy for?

This IT Security Policy applies without exception to all users of Oasis IT Services managed IT facilities and equipment within the Oasis Group. This includes staff, students, contractors and any visitors who have been provided with temporary access privileges.

The policy applies to activities taking place in any location where access to and the use of any Oasis IT systems and/or equipment takes place, e.g. Oasis Laptop computers at home; remote access to any online Oasis systems and/or Microsoft Office 365 and networked resources.

The policy also covers the use of 'Personally Owned Devices' on Oasis premises and their interaction with the Oasis IT System.

4. Policy Statements

4.1 Management of IT Security Risk

4.1.1 The Oasis IT Directorate will maintain a register of IT Security Risks in accordance with the Oasis Risk Management Policy. The risk register will be updated on a monthly basis to ensure changes in the condition of risks are accurately recorded and the status of these risks will be reported to the OCL board.

4.1.2 The introduction of new systems or services and any changes to the IT infrastructure will be risk assessed for the purposes of IT security to ensure that they do not change the risk profile without authorisation.

4.1.3 Mitigations will be applied to reduce both the impact and the likelihood of an IT Security risk being realised to a level acceptable to the OCL board.

4.1.4 Appraisal of risks will be accompanied by a programme of testing to ensure the evaluation of the risks has been accurately interpreted.

4.1.5 Auditing of mitigations will be undertaken to ensure that mitigating actions are in place as detailed in the risk register.

4.1.6 Issues identified will be catalogued and reported as part of the IT Directorate board reporting cycle such that they are escalated to board level, where they can be tracked and monitored.

4.1.7 Controls will be implemented to ensure that the mitigation strategies applied are maintained and cannot be removed without appropriate consideration of the change being undertaken.

4.2 Control Authority within the Oasis IT Infrastructure

4.2.1 Oasis IT Services are responsible for the design, maintenance and day to day management of all Oasis IT Infrastructure. All Oasis Entities must consult with Oasis IT Services before considering any project, programme or change which has an interface with or impacts the IT Infrastructure in anyway. The introduction or change to IT Infrastructure without the approval of the Director of Information Technology is a breach of this policy and may incur further action.

4.2.2 Any Changes to or that impact the IT Infrastructure must be managed according to the Oasis IT Change Management Policy and Process. This includes changes to the physical infrastructure.

4.3 Oasis IT Security Posture

4.3.1 Oasis will achieve and maintain accreditation to the Cyber Security Essentials Security Standard. This policy has been produced in alignment with this standard. Changes to the configuration of the IT system which will cause Oasis to be in breach of this standard will not be permitted.

4.4 Control of Physical Access to the IT Infrastructure

4.4.1 All Physical Infrastructure must be deployed as per the Oasis IT Services Physical Infrastructure Standard.

4.4.2 Spaces housing IT infrastructure must be considered as secure and hence access is restricted to IT and Premises staff. Others, including those representing third party organisations, must be escorted if they have a legitimate need to enter these spaces.

4.4.3 Third party organisations may wish to host infrastructure within Oasis IT infrastructure spaces such as when services are being provided to Oasis premises by the third party. Where this is the case then appropriate security precautions must be taken to ensure that the security and integrity of the network is not compromised. Therefore, hosting of Third-Party solutions must be carried out within the wider requirements of this policy.

4.4.4 Deployed third party hardware must be clearly physically marked and located separately from Oasis infrastructure.

4.4.5 Connections between Oasis infrastructure and third-party solutions must be clearly labelled so they can be easily identified.

4.4.6 The introduction of third-party infrastructure into an Oasis communications space requires a specific risk assessment, considering the security risks of such a deployment and the appropriate mitigations that need to be implemented for sign off by the Director of Information Technology prior to implementation.

4.5 Active Network Infrastructure Security

Network Perimeter

4.5.1 Oasis IT Services is responsible for controlling and managing all interfaces between the IT Infrastructure and other networks including the internet.

4.5.2 Oasis IT Services will maintain a security perimeter at the boundary of the Oasis IT Services Network. Only Oasis IT Services managed connections are allowed into the network. It is a breach of this policy for any external connectivity to be implemented into the Oasis Network that is not fully managed and controlled by Oasis IT Services.

4.5.3 All external interfaces into and out of the Oasis IT infrastructure will be protected by a recognised firewall. Oasis IT Services will configure, maintain and monitor the firewall infrastructure to ensure only authorised connections and traffic are allowed in and out of the network infrastructure.

4.5.4 The Firewall Infrastructure will be configured by Oasis IT Services to restrict the flow of network traffic in and out of the Oasis network. By default, all network traffic will be blocked with specific required classifications of network traffic being allowed to support the effective use of Oasis IT facilities.

4.5.5 Oasis IT Services will monitor the network activity at the network perimeter with the objective of detecting strange and suspicious activity and attempted network intrusions.

4.5.6 Access to the configuration of the network firewalls will be strictly controlled and limited to engineers specifically authorised by the Director of Information Technology. Access to the configuration of the network firewalls will be limited to named engineer accounts associated with individual members of the engineering team which are authenticated via multi-factor authentication.

4.5.7 Changes to the configuration of the network perimeter require a specific risk assessment signed off by a Senior Network Engineer as being a technically accurate reflection of the situation before proceeding to the Change Advisory Board (CAB) for approval.

4.5.8 IT Security and the risk associated with changes will be the primary consideration of the CAB when evaluating changes to the network perimeter.

4.5.9 Any Services that are hosted by Oasis that provide remote access will be deployed with specific security around them to limit the scope of any compromise of that system such that it cannot spread to other systems within the network. This is known as deployment within a DMZ or De-militarised Zone. This includes remotely accessible services which are deployed from local sites and deployments from national data centres.

Use of Virtual Private Networks (VPNs)

4.5.10 Virtual Private Networks are implemented to create secure connections between devices or locations. There are a number of different scenarios for their use which need to be considered separately in this policy. VPNs provide a means for Oasis to connect Oasis locations together, via the public internet in a secure manner (Infrastructure VPN) and a means for individuals to connect back into the Oasis network from their devices, acting as though they are working within the network from a remote location. (Remote Worker VPN). They are commonly used by individuals to hide their activities online, both in terms of the information being accessed and the location from where the access is occurring (Personal VPN). Sometimes third-party providers will offer services to be used by Oasis which require VPN access from within the Oasis IT infrastructure (Third-Party VPN).

4.5.11 Infrastructure VPNs may be used by Oasis as part of the Oasis infrastructure to create links between Oasis sites when configured as per the Oasis Infrastructure VPN standard to provide a safe and secure communications mechanism.

4.5.12 Oasis IT Services do not support Remote Worker VPN services for 'normal' remote access activities. Remote worker services are provided through other means. However, Oasis IT Engineers may make use of VPN connections where there is a specific need to do so, for example where a Remote Worker VPN provides the means to remotely manage infrastructure hardware that cannot be carried out through other remote access mechanisms. Remote Worker VPN access will only be granted with the specific authorisation of the Director of Information Technology.

4.5.13 It is recognised that there can be legitimate reasons for the use of a Personal VPN service, particularly where network infrastructure being used is not trusted. However, personal VPNs prevent Oasis from the legitimate monitoring of communications made within its network infrastructure. Therefore, the use of Personal VPN services from within the Oasis network is prohibited.

4.5.14 Oasis takes advantage of a number of key services which are managed by third parties and which are hosted within the Oasis IT infrastructure. These third parties may request VPN access to manage and maintain these services. Any such access must remain wholly within the control of Oasis IT Services and specifically authorised by the Director of Information Technology.

4.5.15 Third-Party VPN solutions have the potential to introduce significant security risks to the Oasis IT infrastructure. The use of such solutions requires a specific risk assessment that specifically considers how the Oasis IT infrastructure will be protected from these risks and how Oasis will be able to maintain its safeguarding obligations, authorised by the Director of Information Technology prior to implementation.

Network Infrastructure

4.5.16 Only approved network infrastructure equipment will be connected to the Oasis IT Services Managed IT infrastructure.

4.5.17 Additions or subtractions of equipment to the network infrastructure will be managed through the Oasis IT Change Management Policy and Process.

4.5.18 All network infrastructure equipment will be deployed in a manner in keeping with the Oasis IT Services Physical IT Security Standard.

4.5.19 Access for the management network infrastructure components such as switches and routers will be limited to Oasis IT Services Engineers and Oasis IT Services approved contractors and consultants who are appropriately skilled and qualified to do so.

4.5.20 Access for the management of network infrastructure components shall be provided at the discretion of the Director of Information Technology may be removed at any time without notice.

4.5.21 Individual engineers will be provided with access to the network infrastructure through the use of their Microsoft Active Directory Engineering account. Changes to the configuration of the infrastructure will be logged against the account used to implement them.

4.5.22 Log files for changes will be retained as per the Oasis Log File Configuration Standard to allow for the investigation of issues including but not limited to security events.

4.5.23 The network infrastructure will be segmented to the limit the scope of any network compromise. Devices and user access must be via the correct network segment to facilitate access to the services required. The communication between different individual network segments will be limited to the types of communication required for the network to function successfully.

4.5.24 Changes to the network segmentation must be authorised via the Oasis IT Change Management Policy and Process. Consideration of the security implications of such changes will be paramount and these changes will be routinely declined under normal circumstances.

4.5.25 IT Equipment Management interfaces must be deployed within an appropriate secure VLAN (Network Segment) with appropriate Access Control Lists (ACLs) and other restrictions to prevent access to management interfaces from those unauthorised to do so.

Updating Network Infrastructure

4.5.26 Software and Firmware updates are applied to infrastructure hardware to ensure that identified security vulnerabilities and other risks are effectively mitigated.

4.5.27 Network appliance firmware and software must be updated as per the Oasis Network Update and Patching Standard.

4.6 Wireless Network Infrastructure Security

4.6.1 Oasis IT Services will provide a managed wireless network infrastructure for the Oasis Entities within the scope of this policy.

4.6.2 The Oasis Managed Wireless Network Infrastructure provides different wireless networks that have been designed to provide the appropriate access for different devices and user groups.

4.6.3 The Oasis wireless network infrastructure must be configured as per the Oasis Device Connectivity Standard.

4.6.4 'Other' wireless networks, un-managed by Oasis IT Services, are not permitted to link to the Oasis IT Infrastructure.

4.6.5 'Other' wireless networks are not permitted on Oasis premises.

4.6.6 Users and devices must be connected to the correct wireless network in order to be able to gain the correct the access to network services and to maintain network security. Devices and users must be assigned as per the Oasis Device Connectivity Standard

4.7 Server Security

Device Physical Security

4.7.1 Oasis IT Services Service infrastructure such as servers and storage devices will be deployed in a location / environment to meet the requirements of the Oasis IT Services Physical Security Standard.

4.7.2 Physical security features of individual pieces of server hardware must be implemented where they are available. (e.g. lockable server front panels etc)

Operating System Software

4.7.3 Servers within the Oasis infrastructure will only be deployed with supported operating system software.

Server Hardware Firmware Updates

4.7.4 Server hardware requires firmware updates to ensure that it protected from security exploits. Server firmware will be checked each half term to check for new firmware versions for each physical server. Any new firmware that addresses security or critical updates will be applied. Feature and other updates will only be applied if there is an operational need to do so.

Server Operating System and Server Application Software Updates

4.7.5 It is extremely important that Oasis Servers receive software updates to ensure that they kept up to date with fixes and patches to known and newly discovered software vulnerabilities. Oasis IT Services managed devices will have Critical and Security Updates applied to servers as quickly as possible after they are released and validated.

4.7.6 Server software will be updated in accordance with the Oasis Systems Update and Patching Standard

4.7.7 Feature Updates will be applied to operating systems as required

Console Access / Integrated Lights Out Management

4.7.8 Access to the console and or the Integrated Lights Out Management interface on a server provides a powerful means for Engineers to manage and administer a server. However, if not correctly managed, it can create a security vulnerability.

4.7.9 Access to Consoles/Integrated Lights Out Interfaces must be limited to the secure IT Management VLAN (Network Segment).

Security of Information stored on Oasis Servers

4.7.10 Data stored on Oasis Servers must be protected as per the Oasis Information Security Policy

Administrative Access

4.7.11 Administrative Access to Servers must be limited to those members of the Oasis IT Directorate who have a legitimate need to for the access as per the Oasis IT Access Policy.

4.7.12 Access for the management of Server infrastructure shall be provided at the discretion of the Director of Information Technology may be removed at any time without notice.

4.8 Client Device Security

Operating System

4.8.1 Oasis owned devices will only be used with approved operating system software. Approved operating system versions will be supported by the software manufacturer for security updates. The list of currently supported operating systems and versions will be maintained by the National Infrastructure Manager.

4.8.2 All staff portable client devices must be configured to support disk encryption to protect the data in the event of loss or theft of the device.

4.8.3 All new staff client devices must be procured to support hardware-based management of Encryption keys for the device i.e. to include a Trusted Platform Module (TPM) chip or equivalent.

4.8.4 Student devices do not need to include hard disk encryption. However, this means that student devices must not be issued to staff for use, even on a temporary basis. Student devices which may be used by staff members basis must be configured as per a staff device.

Operating System Software Updates

4.8.5 It is extremely important that Oasis devices receive software updates to ensure that they kept up to date with fixes and patches to known and newly discovered software vulnerabilities. Oasis IT Services managed devices will have Critical and Security Updates applied to them as quickly as possible after they are released and validated.

4.8.6 Operating system software updates are managed and applied as per the Oasis Systems Update and Patching Standard.

4.8.7 Feature Updates will be applied to operating systems as required

Client Device Software Firewall

4.8.8 All Oasis client devices must be deployed with a software firewall enabled to prevent unauthorised access to the device.

4.8.9 The software firewall will be enabled at all times including when the devices is connected to the Oasis network. However, it may be that different filtering rules are applied to the device when it is away from the Oasis network.

4.8.10 The software firewall will block incoming communication to the device unless the communication is specifically required for the device to operate successfully.

4.8.11 The firewall must not be user configurable and must be set by policy which is applied to the device.

Local Administrative Access to the Device

4.8.12 Oasis IT Services will maintain local administrative access to all client devices.

4.8.13 It is recognised that some non-IT Staff Users may require local administrative access to a device to allow them to be able to be able to use the device effectively as part of their duties.

However, this administrative access must be granted on the basis of the user account and not on the basis of group membership, therefore meaning specific user accounts are granted administrative access to specific devices.

4.9 Control of Malware

Firewall Anti-Malware Protection

4.9.1 All Oasis internet access must traverse a firewall appliance. Where these firewall appliances include anti-malware protection, it must be enabled to protect the network from the inadvertent or deliberate download of malware onto a device.

4.9.2 Where applicable, a full and active subscription to Anti-malware updates must be maintained to ensure that the latest threats are mitigated at the perimeter of the network as soon as they are discovered by the sector.

4.9.3 Firewall Anti-Malware protection must not be circumvented or disabled for any part of the network other than for the purposes of troubleshooting and problem management by the Oasis IT Team.

4.9.4 Any changes to the firewall Anti-Malware configuration, including temporary changes for troubleshooting purposes are considered a national change and must be so managed via the IT Change management policy.

Web Filtering Anti-Malware Protection

4.9.5 All Oasis internet access is filtered through a filtering appliance. The filtering rules on these appliances must be configured as the Oasis Web filtering Policy.

4.9.6 Anti-Malware features of the web filtering appliances must be enabled to protect the network from the inadvertent or deliberate download of malware onto a device.

4.9.7 Where applicable, a full and active subscription to Anti-malware updates must be maintained to ensure that the latest threats are mitigated at the perimeter of the network as soon as they are discovered by the sector.

4.9.8 Web Filtering Anti-Malware protection must not be circumvented or disabled for any part of the network other than for the purposes of troubleshooting and problem management by the Oasis IT Team.

4.9.9 Any changes to the Web Filtering Anti-Malware configuration, including temporary changes for troubleshooting purposes are considered a national change and must be so managed via the IT Change management policy.

Windows Device Anti-Malware Protection

4.9.10 All Oasis Microsoft Windows client devices and Servers must be protected by Oasis IT Services approved anti-malware software.

4.9.11 All Oasis Anti-Malware software must be updated daily.

4.9.12 The anti-malware software will be configured as per the Oasis Anti-Malware client configuration standard.

4.9.13 The anti-malware software must not be user configurable and the setting must be configured by policy.

Cloud based Anti-Malware Protection

4.9.14 Oasis client devices will be configured to make use of cloud based Anti-Malware protection wherever they are deployed.

4.9.15 Oasis IT Services devices may not be configured to make use of Cloud based Anti-Malware protection solution for a range of purposes associated with the role of the individual and device including administration and testing of the IT solution and the security risks.

4.10 Control of User Access (Authentication)

Authentication

4.10.1 Microsoft Active Directory is considered to be the primary method to authenticate users of Oasis IT resources including Oasis IT Engineers gaining access to specific infrastructure hardware and software.

4.10.2 All Oasis IT services (including those not managed by Oasis IT Services) that are accessible from the internet will be authenticated using the users Microsoft Active Directory Account.

4.10.3 IT Services that are not accessible from the internet may use an authentication solution that is built into the platform. However, access to these systems must require authentication against the Oasis Active Directory infrastructure in order to be able to obtain access to the solution i.e. must require authentication to an Oasis device or via Remote Desktop Services.

4.10.4 Multi-Factor Authentication will be implemented for all Oasis Staff members who have general access to the IT system. User access for staff members with limited access can be implemented without the implementation of Multi-factor authentication with the specific authorisation of the Director of Information Technology. For the purposes of this policy, limited access excludes access to any shared drives, management information or finance systems or any system or location which stores personal or special category information about an individual.

4.10.5 Where a non-staff member requires access to the Oasis network for purposes of working with Oasis (e.g. for student teachers, supply teachers, temporary staff, contractors etc) then they will be required to have Multi-factor authentication enabled for their account unless the required access is limited as per 4.10.4.

Third Party Service Integration/Federation

4.10.6 It is recognised that third party solutions may be deployed that require authentication against the Oasis Microsoft Active Directory user account system. This can be implemented where the third-party solution is assessed by the Director of Information Technology to preserve the integrity and security of the Oasis IT solution.

4.11 Control of Installed Software

Procurement of Software

4.11.1 The selection and procurement of software must be undertaken in consultation with Oasis IT Services. Software procured outside of this route may not be installed or compatible and therefore could result in a waste of public money.

4.11.2 Purchase of new software solutions requires specific technical authorisation by Oasis IT Services as detailed in the 'Scheme of Delegation.'

4.11.3 The 'Technical Authorisation' process shall give due consideration to the security implications of the introduction of the software including but not limited to whether the software has any external access interfaces.

Installation of Software

4.11.4 Only authorised software can be installed on Oasis owned and managed devices. Any authorisation will give due consideration to the IT Security risks that the installation of the software may present.

4.11.5 Oasis IT Services will manage the software installed on individual devices and servers.

4.11.6 Users must not install software onto a device without authorisation from the Oasis IT Services team, recorded through an OCMS service request.

4.11.7 Authorisation for the use of software may be withdrawn at any time in response to identified security vulnerabilities. Where authorisation is withdrawn, the software may be removed from the Oasis IT Infrastructure immediately.

Software Updates / Versions

4.11.8 It is important that software installed on Oasis devices and servers does not present an opportunity for the compromise of the IT system. It is therefore important that software updates are applied to address security vulnerabilities in applications.

4.11.9 Obtaining updates may require service and support agreements to be in place. Software owners are required to ensure that any such service and support agreements are maintained.

4.11.10 Where appropriate updates to address identified security risks cannot be obtained, including where software is no longer supported by the developer or where the support agreement is not in place, the software may be removed from the Oasis IT Infrastructure immediately.

4.11.11 The use of unsupported software versions could restrict the updates / versions of system software implemented in the wider infrastructure in-order to maintain compatibility. Maintaining this compatibility will not be considered a reason for delaying or not implementing infrastructure / platform system updates and version progression.

4.12 Management of Passwords

4.12.1 Individual passwords must be created to comply with the Oasis Password Policy including those used to support IT Engineering, Service and System accounts.

4.12.2 Oasis IT Services needs to create and maintain passwords for service and other administrative accounts. The details of these accounts must be recorded the Oasis IT Services Password Management System.

4.12.3 Access to the password manager system will be restricted to Oasis IT Services engineers, Contractors and Consultants who have a need to have access to the password manager system.

4.12.4 Access to the password manager will be controlled such that only the passwords relating to those systems which an IT Engineer has a legitimate need access/manage/support will be available to them.

4.13 Third Party Organisations making use of Oasis IT Infrastructure

4.13.1 Third party organisations such as tenants or other users of Oasis buildings, must not be granted general access to the Oasis IT Infrastructure. Access by third party organisations must be through the provision of dedicated facilities for these organisations within the infrastructure.

4.13.2 Oasis IT Services will provide fully segregated network provision for the third-party organisation within the Oasis IT infrastructure that will prevent access to Oasis data or services but allow the Third Party to operate within the Oasis site.

4.13.3 Oasis IT Services will make internet connectivity available through the Oasis management internet connections to the third-party organisations making use of the infrastructure. Third Party Organisations are not permitted to provide their own internet connections into Oasis Premises unless specifically authorised by the Director of Information Technology to do so.

4.13.4 Oasis IT Services can provide a wireless network infrastructure for the third-party organisation. The network will be configured as a dedicated wireless SSID and integrated into the wired VLAN for the third-party organisation.

4.13.5 Oasis IT Services will re-charge the Oasis Entity for the provision of services for third parties. The Oasis Entity may choose to recharge the third party for the use of the service.

4.14 Cyber Café's and other Public Access

4.14.1 Devices that are provided for public use must be fully segregated from the Oasis network, only providing access to the internet but preventing access to all other Oasis systems and services.

4.14.2 Public access devices must be configured as per the Oasis Device Connectivity Standard.

4.14.3 Oasis Entities may wish to provide access to the internet for members of the public. The default method of providing this access is via the Oasis Guest Managed Wireless Infrastructure. However, if wired network access is required then additional specific configuration will need to be put into place to accommodate the access. This will be considered as an IT project and there may be costs associated with the provision to be met by the requesting Oasis Entity.

4.15 Testing and Audit of IT Security

Monitoring Physical Security

4.15.1 Annual Monitoring and inspection of the Physical security of the Oasis IT estate will be undertaken as part of the Quality Assurance Process. The Physical Security Audit will be undertaken in comparison to the Oasis IT Physical Security Standard to identify where the requirements are not being met by any part of the deployed infrastructure.

Penetration Testing

4.15.2 Oasis IT Services will commission a suitably qualified, third party to undertake annual penetration testing of the Oasis IT system. The detail of the penetration testing will reflect the

work that has been undertaken and changes to the system made over the previous year but will be sufficient in scope to identify common security weaknesses of the infrastructure to both internal and external threats.

User Awareness Testing/Training

4.15.3 Oasis IT Services will undertake periodic tests of user awareness to Phishing, Spear Phishing attacks and other types of Cyber-attacks which are triggered by user interaction. Such tests will be conducted as realistically as possible without jeopardising the security of the IT infrastructure

5. The requirements that apply to this policy

Related Oasis Policies, Standards and Processes

This policy should be read in conjunction with the following Oasis Policies:

- The Oasis Device Monitoring Policy
- The Oasis Web Filtering Policy
- The Oasis Data Protection Policy
- The Oasis IT Password Policy
- The Oasis IT Access Policy
- The Oasis Information Security Policy
- The Oasis IT Major Investigation Policy
- The Oasis IT Services Change Management Policy
- The Oasis Systems Update and Patching Standard
- The Oasis IT Services Physical Security Standard
- The Oasis Device Connectivity Standard.
- The Oasis Infrastructure VPN standard
- The Oasis Community Learning Scheme of Delegation

Applicable Legislation, Guidance and References

The user must comply with all the relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Data Protection Act 2018.

RACI Matrix

R = Responsible A = Accountable C = Consulted I = Informed

Policy Element			Leadership									IT Team								
	Policy Owner	IT System User	Group CEO	OCL CEO	OCL COO	National Director	Regional Director	Academy Principal	Designated Representative	Head of National Service	Data Protection Officer	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of IT Strategic Projects	Service Desk Manager	National Service Desk	Service Delivery Manager	Cluster Manager	Onsite IT Teams
4.1 Management of IT Security Risk					I			I			C	A	R	R	R	R	R	I	I	I
4.2 Control Authority					C	C	C	C	C	C	C	A	R	R	R	R	R	R	R	R
4.3 IT Security Posture				C	C	C	I	I	I	I	I	A	R	R	R	R	R	R	R	I
4.4 Physical Access				I	C	I	C	C	I	I	C	A	R	R	R	R	R	R	R	R
4.5 Active Network Infrastructure Security				I	C	I	I	I	I	I	C	A	R	R	R	R	R	I	I	I
4.6 Wireless Network Infrastructure Security				I	C	I	I	I	I	I	C	A	R	R	R	R	R	I	I	I
4.7 Server Security					C			I	I	I	C	A	R	R	R	R	R	R	R	R
4.8 Client Device Security		I		I	C			I	I		C	A	R	R	R	R	R	R	R	R
4.9 Control of Malware		R			C			R	C	R	C	A	R	R	R	R	R	R	R	R
4.10 Authentication		I		I	C	I	I	I		I	C	A	R	R	R	R	R	I	I	I
4.11 Control of Installed Software					C		C	C	C	C	C	A	R	R	R	R	R	R	R	R
4.12 Management of Passwords											C	A	R	R	R	R	R	R	R	R
4.13 Third Party use of the Oasis IT Infrastructure			C	C	C	I	C	C	I	C	C	A	R	R	R	R	R	C	C	I
4.14 Cyber Café's and other Public Access			C	C	C	I	C	C	I	C	C	A	R	R	R	R	R	C	C	I
4.15 Testing and Audit of IT Security			I	I	C						C	A	R	R	R	R	R	R	R	R

Document Control

Changes History

Version	Date	Owned and Amended by	Recipients	Purpose
1.0	July 2019	Rob Lamont		First Draft
1.1	Oct 2019	Rob Lamont		For Comment
1.2	Dec 2019	Rob Lamont		For Comment
1.3	Jan 2020	Rob Lamont		First Release
1.4	April 2021	Rob Lamont		Formatted to new template

Policy Tier

☐ Tier 1
☒ Tier 2
☐ Tier 3
☐ Tier 4

Owner

Director of Information Technology

Contact in case of query

Rob.Lamont@Oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
Directors Meeting		05.07.21	1.5

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: Internal IT Directorate Documentation

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