USE OF PERSONALLY OWNED DEVICES POLICY (UPOD)

October 2019

CONTENTS

1.0 Introduction

Oasis's mission is to transformation of communities. This work involves the use of an extensive range of technology and an extensive use of Oasis owned and managed IT infrastructure. Oasis staff are committed to this mission and often go above and beyond what is expected, this includes choosing to use IT equipment that they themselves have provided rather than making use of the devices that Oasis provides for the purpose of undertaking this work. Oasis do not mandate the Use of Personally Owned Devices and provide equipment that is sufficient to allow them to undertake their work. However, we recognise that some users may prefer to use other equipment and therefore we wish to provide a solution to allow this to happen in a safe and secure 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. From time to time, we may amend this policy, the current version will be available on the Oasis Policy Portal. Requests to change the policy should be made to the Director of IT Services. The policy has been developed in the context of the Oasis Ethos and Nine Habits of behaviour.

2.0 What is this policy about?

The purpose of this policy is to provide guidance on the permitted Use of Personally Owned Devices connecting to the Oasis network including the use of any online Oasis systems and/or the Oasis managed Microsoft Office 365, the internet, e-mail, instant messaging, social media, media publications, file transmission and voice communications and includes the use of personally owned devices at home for remote access.

Policy Scope

The Use of Personally Owned Devices (to be known as UPOD) is only permitted for users who hold an existing Oasis IT Services User Account. It should be interpreted such that it has the widest application and to include new and developing technologies and uses, which may not be explicitly referred to.

This policy applies to all users of the Oasis Services Managed IT infrastructure including users within 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

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

This policy applies to both the use of personally owned devices on Oasis premises (BYOD) and the Use of Personally Owned Devices away from Oasis premises for the purposes of remote access. 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. laptop computers at home; remote access to any online Oasis systems and/or Microsoft Office 365 and networked resources.

Policy Principles

Oasis employees who make use of personally owned devices do so because they choose to and are not compelled to provide devices for use in business related activities in any way.

Oasis seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting users with highest possible system standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of Oasis.

Where users are permitted to use their own devices, they will be deemed to be familiar with and bound by this UPOD policy and the Oasis Acceptable Use of Technologies Policy (AUTP). A copy of these policies can be found on the Oasis Policy Portal.

In addition to this UPOD Policy, users working within educational context and with Oasis IT systems are required to comply with the Oasis E-Safety Policy and should note that the contents of this document are fully compliant with the DfE statutory guidelines 'Keeping children safe in education'.

Oasis also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Oasis will implement Web Filtering including monitoring as detailed in the Oasis Web Filtering Policy which will impact Personally Owned Devices used within the Oasis IT infrastructure. Users should note that it will not be possible for Oasis to filter internet access on Personally Owned Devices when outside of the Oasis system, e.g. at home.

Oasis will keep the UPOD Policy updated to match all applicable legislation re personal use of technologies and as becomes statute. Updated versions will be available through the Oasis Policy Portal.

Policy Objectives

The objectives of this policy are to:

- Define the acceptable and unacceptable uses of personal devices connected to Oasis IT systems.
- Define how use will be monitored in conjunction with the Oasis Device Monitoring Policy Define how requests for access will be dealt within the Oasis IT Access Policy.
- Define consequences for misuse

Policy Strategy

This policy has been developed to ensure that Oasis users are able to make use of Personally Owned Devices with the Oasis IT Services managed IT infrastructure and services, when they are authorised to do so, in a manner which ensures the privacy of Oasis Data Subjects and the security of the Oasis IT system.

The policy has been developed to allow authorised users of the Oasis IT System to feel confident that the safeguarding of staff, the young and vulnerable people within our care, wider legal responsibilities and the need to effectively manage our IT services whilst respecting and maintaining the privacy of our users have all been met.

For Oasis staff, the Oasis management/leadership will provide the equipment required to undertake their role. The level of equipment provided will be at the discretion of Oasis but equally will be sufficient to allow staff to do their jobs. The use of personally owned devices must be authorised by line manager.

This UPOD Policy includes the use of email on personal devices including phones. Note should be taken that the Oasis Information Security Policy details the way security will be forced onto portable devices if they connect to the Oasis email system.

Oasis staff that have access to personal data, are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

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 E-Safety Policy
- The Oasis Password Policy
- The Oasis Confidentiality Policy
- The Oasis Community Learning Safeguarding Policy
- The Oasis Acceptable Use of Technologies Policies
- The Oasis IT Security Policy
- The Oasis Information Security Policy
- The Oasis IT Major Investigation Policy
- The Oasis IT Access Policy
- The Oasis IT Services Change Management Policy

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:

- Copyright, Designs and Patents Act 1988;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Criminal Justice and Public Order Act 1994;
- Trade Marks Act 1994;
- Data Protection Act 2018;

- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;
- Communications Act 2003;
- Criminal Justice and Immigration Act 2008.
- Keeping Children Safe in Education 2019
- The PREVENT Duty for Schools and Childcare providers

Any breach of the above legislation or related polices is considered to be an offence and in that event, Oasis Community Learning's disciplinary procedures will apply.

Definitions

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

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: A system used to record safeguarding related activity on a client device.

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 user account is the basic identifier through which access is allowed or denied. User accounts are associated with a named person. The association may be 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.

3.0 Application of this Policy

3.1. UPOD - Acceptable Use of Technologies Agreement

3.1.1. Before being granted permission for using their own device a user must accept the Acceptable Use of Technologies Agreement as set out in the Acceptable Use of Technologies Policy (AUTP). These Policies cover both use within and outside of Oasis environments, including home use.

3.1.2. Oasis has a set of default Acceptable Use of Technologies Agreements for different age groups with age appropriate text that form part of the E-Safety Policy and should be used where any UPOD functionality is agreed within an Oasis Entity.

3.1.3. Any issues relating to the restrictions set within these documents should be discussed with the Oasis IT Services team via the Service Delivery Manager.

3.2. Monitoring

3.2.1. Access to the system by personally owned devices (UPOD) is monitored. Monitoring is conducted under the provisions of the Oasis Device Monitoring Policy.

3.2.2. It should be noted that the Use of Personally Owned Devices cannot be fully actively monitored in the same manner as Oasis equipment.

3.2.3. If Oasis, including Oasis IT Services, inadvertently discovers content on a personally owned device that has been introduced to the Oasis network, that brings into question the conduct, standards of behaviour and the outworking of the Oasis Ethos, this will be brought to the attention of the organisation and may lead to disciplinary action

3.3. Device setup for personally owned devices on Oasis System

3.3.1. **Connectivity**

The Use of Personally Owned devices within the Oasis infrastructure requires an individual to have been issued staff, student access to the network. Connectivity is provided according to compliance with the following statements

3.3.1.1. Use of Oasis IT facilities and services on a personally owned device will be deemed to be acceptance of the terms and conditions of this policy. All Users of Oasis IT systems are required to accept this policy and are conversant with and have agreed to the Oasis Acceptable Use of Technologies Policy.

3.3.1.2. A personally owned device brought into the network can only be used on the 'BYOD' wireless network. Student access to the BYOD network for users' to be specifically authorised by the appropriate Academy Principal. All staff are permitted to access the 'BYOD' network by default.

3.3.1.3. Oasis IT Services do not support the use of UPOD on wired networks or on other wireless networks.

3.3.1.4. Where necessary contract technical staff working for the IT department would be allowed to access other wired networks beyond the 'BYOD' network at the sole discretion of the Director of IT Services.

3.3.2. **Security**

3.3.2.1. The minimum-security standards for personally owned devices that are used with Oasis services and data is set out in the within the Oasis Information Security Policy. The standards apply equally to Oasis owned and Personally owned devices. Users are accountable for ensuring their devices meet these standards

3.3.3. **Oasis Data including Personally Identifiable Information**

3.3.3.1. It is not recommended that Personally Identifiable Information is stored on a personally owned device that will be used in connection with work activities on the Oasis system. Where users do make use of Personally Owned Devices, they are accountable for ensuring that appropriate security and safeguards are in place that meet the requirements of the Oasis Information Security Policy.

3.3.3.2. Access to devices which contain Oasis Data must be controlled, this includes access to devices by family members or friends. The user is accountable for ensuring that Oasis Data stored on Personally Owned Devices is only accessed by individuals who are authorised to access the data.

3.3.3.3. Users agree to delete any Oasis related data which has been stored onto a Personally Owned Device when it is no longer actively required and when a user leaves the organisation or when so directed by an authorised Oasis representative.

3.3.3.4. Users are required to keep Oasis Data separate from Personal Data.

3.3.3.5. The Oasis Information Security Policy requires that Oasis Data stored on personally owned devices is synchronised to Oasis systems.

3.3.4. Software Licenses

3.3.4.1. Any software used on personally owned devices for work related purposes needs to be appropriately licensed for business use by the user, including the operating system. Oasis has the right to report any illegally downloaded software that is inadvertently found on a personally owned device used in conjunction with Oasis system. Oasis will hold staff members personally liable for any costs arising from the use of illegal software on personally owned devices in undertaking work on behalf of Oasis.

3.3.4.2. Microsoft Office is provided to users by Oasis as part of the agreed O365 access. No other Oasis software will be installed on a user's personally owned device for work activities.

3.3.5. Accessing Oasis system from external locations on personally owned devices

3.3.5.1. On entry to some countries, a user may be compelled to provide their username and password to a device for inspection in order to be granted entry into the country. This would contravene the Oasis Data Protection Policy.

3.3.5.2. To mitigate this risk, when undertaking foreign travel, users of personally owned devices must ensure that any Oasis data is removed from the device prior to leaving the United Kingdom.

3.3.5.3. Use of public WiFi can require the installation of security certificates which in turn allow the WIFI provider to intercept and monitor the content of emails and use of the internet. The Oasis Information Security Policy sets out the requirements for the use of public WIFI which apply equally to Oasis owned and Personally Owned Devices when they are being used for the processing of Oasis Data.

3.3.6. Technical Support for Personally Owned Devices

3.3.6.1. Oasis IT Services will not provide support for use Personally Owned Devices. Where possible Oasis IT Services personnel will provide advice in the use of Personally Owned Devices without guaranteeing to resolve support queries including those relating to making personally owned devices work with the Oasis system.

3.3.6.2. Users should continue to log call with the Oasis IT Service Desk if the issue is related to the Microsoft Office 365 environment

3.4. Unacceptable use of personally owned devices and Oasis network

3.4.1. Users should refer to the Agreement in the Oasis Acceptable Use of Technologies Policy for details of what is unacceptable use of both Personally Owned Devices within the Oasis network and that are used to process Oasis data and Oasis owned equipment including for reference to exceptions for Personally Owned Devices.

Appendix 1 – RACI Matrix

Policy Element		Leadership				Academy						Services											
	Policy Owner	Group CEO	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Data Protection Lead	Teacher	Academy User	Students	Head of National Service	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Head of IT Strategic Projects	IT Business Operations Manager	Data Protection Officer	Service Desk Manager	National Service Desk	Service Delivery Manager	Cluster Manager	Onsite Teams
Scope, Principles, Objectives, References	A			I										R									
3.1. UPOD Acceptable Use of Personally Owned Devices Agreement (Academy & National)				I	C	R	I	C	I	A	A	I	A	R	I	I	I	I	C	I	I	C	I	I
3.2 Monitoring (Academy & National)				I	C	R	I	C	I	I	I	C	I	A	I	C	I		C	I	I	R	I	I

3.3.1 Connectivity of personally owned devices (Academy & National)				I	I	I	I	I	I	I	I	I	I	A	C	C	I		I	I	I	R	I	I
3.3.2 Security settings on personally owned devices (Academy & National)				I	I	I	I	I	I	A	A	I	A	C	C	C	I		C	I	I	R	I	I
3.3.3 Personally identifiable data (Academy & National)				I	I	I	I	C	I	A	A	I	I	C	C	C	I	I	C	C	I	C	C	C
3.3.4 Software licences (Academy & National)				I	I	I	I	I	I	A	A	I	A	C	C	C	I	C	C	C	I	C	I	I
3.3.5 Accessing from external locations				C	C	I	I	I	I	A	A	C	A	C	C	C	I	I	C	I	I	C	C	C
3.3.6 Support for personally owned devices				I	I	I	I		I	I	I	I	I	A	I	I	I	I	I	I	I	R	C	I
3.4 Unacceptable use of personally owned devices				I	I	I	I	I	I	A	A	I	A									C		
Appendix 2 - Reference - Legal Constraints	A			I										R										
Appendix 3 – Reference - Use of Personally Owned Devices Agreement	A			I										R										

Appendix 2 Reference - Legal Constraints

Copyright, Designs and Patents Act 1988
This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Malicious Communications Act 1988
Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally, under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

Computer Misuse Act 1990
This Act makes it an offence

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities; maliciously to corrupt or erase data or programs; to deny access to authorised users.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:-

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994
This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

Data Protection Act 2018
Oasis Trust has a comprehensive Data Protection Policy, of which the following statement is the summary:

- Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat it in an appropriate and lawful manner.
- The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, stakeholders and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

- This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action.
- Oasis Community Learning and the academies it manages and maintains believe that protecting the privacy of our staff and pupils and regulating their safety through data management, control, and evaluation is vital to both academy and individual progress. The academies collect personal data from pupils, parents, and staff and process it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.
- We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the academy will keep parents fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the academy needs. Through effective data management we can monitor a range of academy provisions and evaluate the wellbeing and academic progression of our academy body to ensure that we are doing all that we can to support both staff and students.

Human Rights Act 1998

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the Oasis Trust, important human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The Oasis Trust, together with all users of its IT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted, in order to:

Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system; Prevent or detect crime or in the interests of national security; Ensure the effective operation of the system.

Freedom of Information Act 2000

The Act, intended to increase openness and transparency, obliges public bodies, including Educational Institutions, to disclose a wide range of information, both proactively and in response to requests from the public. The information held that may be released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such the nature of the information request. In addition to setting a new standard

of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore, all staff have a responsibility to know what information they hold and where and how to locate it.

Communications Act 2003
This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

Criminal Justice and Immigration Act 2008
This act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations 'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage, but failed to take reasonable steps to prevent the contravention.'

Keeping Children Safe in Education 2019
This is statutory guidance from the Department for Education (the department) issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children.This means that they should comply with it unless exceptional circumstances arise.

Prevent
The Prevent strategy has been re-focused following a review. The strategy now contains three objectives: to respond to the ideological challenge of terrorism and the threat from those who promote it; to prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and to work with sectors and institutions where there are risks of radicalisation that we need to address.

Appendix 3 Reference – Use of Personally Owned Devices Agreement

Users must comply and agree with the Acceptable Use of Technologies Policy and Agreement before they can make use of personally owned devices. Should they choose to use personally owned devices they must also agree to this UPOD Agreement.

These are the Terms and Conditions for the Use of Personally Owned Devices and are intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- Oasis IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of IT in their everyday work.
- Oasis will try to ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for student learning and will, in return, expect staff and volunteers to agree to be responsible and accountable users:
- I understand that I must use Oasis IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.
- I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT.
- I will, where possible, educate the students in my care in the safe use of IT and embed ESafety in my work with students.

For my professional and personal safety:

- I understand that Oasis will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Oasis IT systems (e.g. devices provided by Oasis for my personal use, personally owned devices, laptops, mobile phones, email, Microsoft Office 365 and related tools) inside and outside of academy sites.
- I understand that Oasis IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Oasis.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Oasis IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with Oasis policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. Microsoft Office 365 and tools) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in Oasis in accordance with the Oasis policies.
- I will only communicate with students and parents / carers using official Oasis systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Oasis has the responsibility to provide safe and secure access to technologies and ensure the smooth running of Oasis:

- When I use personally owned devices (e.g. hand held / external devices- PDAs / laptops / mobile phones / USB devices etc.) in Oasis, I will follow the rules set out in this agreement, in the same way as if I was using Oasis equipment. I will comply to the Oasis Use of Personally Owned Devices Policy (UPOD)
- I will not use personal email addresses on the Oasis IT systems.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is saved on the Oasis network and where this is not possible that it is backed up, in accordance with relevant Oasis policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to inappropriate materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Oasis Data Protection and Information Security Policies (or other relevant Oasis policy). Where personal data is transferred outside the secure Oasis network, it must be encrypted.
- I understand that Oasis Data Protection and Information Security Policies require that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Oasis policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Oasis sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and outside of Oasis.
- I understand that this Acceptable Use Agreement applies not only to my work and use of Oasis IT equipment in Oasis, but also applies to my use of Oasis IT systems and equipment out of Oasis and my use of personally owned equipment in and outside of Oasis or in situations related to my employment by Oasis.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to formal disciplinary action which may include a warning, suspension and/or summary dismissal for gross misconduct dependent on the severity of the offence. I also understand that Oasis will report any illegal activities to the police and/or any other relevant statutory authority

I have read and understand the above and agree to use Oasis IT systems (both in and out of Oasis) and on my personally owned devices (in Oasis and when carrying out communications related to Oasis) within these guidelines.

Document Control

Changes History

Version	Date	Owned and Amended by	Recipients	Purpose
0.1	November 2017	Liz Hankin	IT Policy Working Group	1st draft
0.2	December 2017	Liz Hankin	IT Policy Working Group	Updated following Feedback
0.3	December 2017	Liz Hankin	IT Policy Working Group	Final draft version ready for Rob L to edit.

1.0	December 2017	Rob Lamont	John Barneby, Dave Parr	Final Draft for Approval
1.1	June 2018	Sarah Otto	John Barneby, Dave Parr	Final Draft for Approval
1.2	August 2019	Marc Hundley		Reviewed content, migrated to new Policy template
1.3	October 2019	Marc Hundley		Updated layout, updated legislation to current versions
1.4	October 2019	IT Business Relationship Manager, Marc Hundley	Director of IT, Rob Lamont	For Approval

Policy Tier

☐ Tier 1

☐ Tier 2

☒ Tier 3

☐ Tier 4

Owner

IT Business Relationship Manager, Marc Hundley

Contact in case of query

Marc.hundley@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
Rob Lamont	Director of IT	30th October 2019	1.4

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 Policy Portal		21.11.19	V1.4
