# ACCEPTABLE USE OF TECHNOLOGIES POLICY

**May 2019**

CONTENTS

## 1.0 Introduction

Technology provides a critical infrastructure that supports us in our work transforming communities. New technologies have become integral to the lives of children, young people and adults in today's society, both within Oasis and in their lives outside. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone.

The use of Information Technology enhances our productivity and helps us to communicate effectively. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. However, this use of Technology needs to be undertaken in a way that maximises the benefits, ensures that the infrastructure is not abused and is available to use.

The purpose of this policy is to provide guidance on the use of Oasis IT Services Managed network resources which includes the use of any online Oasis systems and/or Microsoft Office 365, the internet, e-mail, instant messaging, social media, media publications, file transmission and voice communications. 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 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. Requests to change the policy should be made to the Director of IT Information Technology. The policy has been developed in the context of the Oasis Ethos and Nine Habits of behaviour.

## 2.0 What is this policy about

### Policy Scope

This Acceptable Use of Technologies Policy (AUTP) applies without exception to all users of Oasis IT Services Managed ICT facilities and equipment within the Oasis Group. This includes staff, students 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. 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.

Oasis Community Learning has a set of default Acceptable Use of Technologies Agreements for different age groups, making use of age appropriate wording that form part of the Oasis E-Safety Policy.

### Policy Principles

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. All users will be deemed to be familiar with and bound by this AUTP. A copy of the current version of this policy can be found on the Oasis SharePoint Policy Portal.

Users/ staff working within educational context and with OCL 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 keep the AUTP updated to match all applicable legislation re personal use of technologies and as becomes statute. Versions of any updated versions will be available through the Oasis Policy Portal.

### Policy Objectives

The objectives of this policy are to:

- Ensure that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- Ensure that Oasis IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Ensure that staff and students are protected from potential risk in their use of IT in their everyday work.
- Define the acceptable and unacceptable uses of Oasis IT Services Managed ICT systems.  Define how use will be monitored in conjunction with the Oasis Device Monitoring Policy.

## 3.0 Application of this policy

### Policy Strategy

The policy has been developed to allow users of the Oasis IT System to feel confident that 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.

To ensure the acceptable use of Oasis systems, Oasis IT Services will monitor email, telephone and any other electronically-mediated communications, whether stored or in transit, in line with relevant legislation. Further details of the monitoring that is undertaken is given in the Oasis Device Monitoring Policy and the Oasis Web Filtering Policy. All users of Oasis ICT facilities or equipment expressly waive any right of privacy and therefore should have no expectations of privacy in anything they create, store, send or receive using Oasis' ICT systems and equipment.

To use Oasis IT facilities, a person must have been issued staff, student or guest access to the network. Use of Oasis IT facilities 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. All users of the Oasis IT Services Managed IT Systems will be deemed to be familiar with and bound by this AUTP.

All users will adhere to the Oasis Password Policy and guidelines and Oasis Data Protection Policy in addition to all relevant regulatory and legal requirements. Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken.

Oasis staff that have access to personal data, as defined in appropriate legislation, 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 in accordance with the Oasis Data Protection, Oasis Confidentiality and the Oasis Information Security Policies.

## 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 Email Policy
- The Oasis E-Safety Policy
- The Oasis Community Learning Safeguarding Policy
- The Oasis IT Access Policy
- The Oasis IT Security Policy
- The Oasis Information Security Policy
- The Oasis IT Major Investigation Policy
- The Oasis IT Services Change Management Policy
- The Oasis IT Services Incident Management Policy
- The Oasis Confidentiality 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 2016
- The PREVENT Duty for Schools and Childcare providers

## Definitions

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

**Future Cloud:** See PCE

**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

**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.

## 4.0 Policy Statement

### 4.1. Terms of Use

4.1.1. Use of the Oasis IT System is undertaken in compliance with the Oasis IT System, Terms of Use, which set out the conditions under which access to the IT system is provided.

4.1.2. The 'Terms of Use' of the Oasis IT system can found in Appendix 2 – 'Terms of Use of the Oasis IT System'

4.1.3. The 'Terms of Use' apply to the Oasis IT System uniformly, individual Oasis entities must not adopt individual 'Terms of Use.'

4.1.4. By accessing Oasis IT systems and resources, Users agree to adhere to the 'Terms of Use of the Oasis IT System.' Failure to adhere to these 'Terms of Use' is a breach of this policy.

4.1.5. Where possible, Users will be required to accept the 'Terms of Use' when accessing the system. As a result of technical limitations of some systems this will not always be displayed. Users accessing the system are deemed to have accepted the Terms of Use regardless of if they are displayed prior to logon.

4.1.6. All users of Oasis IT systems or equipment expressly waive any right of privacy and therefore should have no expectation of privacy in anything they create, store, send or receive using Oasis' IT systems and equipment.

### 4.2. Access to the Oasis IT System

4.2.1. Access to the Oasis IT System is granted in accordance with the Oasis IT Access Policy.

4.2.2. User accounts are used to facilitate access to the IT System.

4.2.3. Users must not facilitate access to the system using their users accounts to others, including by providing their username and password to others or by logging other users onto the system using their account.

4.2.4. Users are accountable for the protection of their account details and for the actions undertaken with their user account.

### 4.3. Monitoring

4.3.1. Monitoring of use of the Oasis IT System is conducted in accordance with the Oasis Device Monitoring Policy.

4.3.2. Access to the system for use of personally owned devices is monitored in accordance with the Oasis Use of Personally Owned Devices (UPOD) Policy.

4.3.3. Within this Acceptable Use of Technologies Policy monitoring will include:

4.3.4. To ensure that the safeguarding of young people and vulnerable adults is maintained.

4.3.5. To maintain a record of events that have occurred where evidence may be required at a later date. (e.g. to provide evidence of commercial transactions in cases of disputes);

4.3.6. Investigate or detect unauthorised use of group telecommunications systems and ensure compliance with this policy or other Oasis policies;

4.3.7. Prevent breach of the law or investigate a suspected breach of the law, the Oasis polices or contracts;

4.3.8. Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);

4.3.9. Monitor standards including the performance and availability of the system and ensure effective quality control.

4.3.10. Monitoring may include but is not limited to:

4.3.11. Logon and logoff events against user accounts to record when a user account was in use, including the nature of activities undertaken, the devices used, and the software and services accessed.

4.3.12. The utilisation of device activity monitoring software (PCE) to record activity undertaken on a device. This allows the activity on the device to be recorded and played back in the course of an investigation and provides active monitoring and alerting of device use against potential safeguarding concerns.

4.3.13. The monitoring of specific usage of line of business applications including the login and log off to the systems, the access/changes undertaken and the locations/devices that the access was undertaken from.

4.3.14. The monitoring of Internet sites visited by individual users, including information downloaded from the internet, the level of utilisation, the timing of the activity, the location/device that the activity occurred from and the categorisation of sites visited including reporting on attempted breaches of filtering;

4.3.15. The use of email including the number and frequency of emails sent and received, including viewing sent or received emails from a particular mailbox or stored on any server;

4.3.16. The recording of instant message communication through the Skype for Business and Teams services.

4.3.17. IT System, Server, Firewall, Infrastructure and device system logs which record the utilisation of the systems by users.

## 4.4. Unacceptable use of the Oasis IT System

4.4.1. The Oasis IT System is provided for members of the Oasis family to undertake their duties in pursuit of the organisations vision to support community. Users should always consider the spirit of the Oasis Ethos and the lens of the 9 habits when working on Oasis IT systems. Any conduct which may discredit or harm Oasis, its staff or the IT facilities or can otherwise be considered intentionally unethical or is contrary to our Ethos 9 Habits is deemed unacceptable.

4.4.2. Specific unacceptable use of the Oasis IT System may include but not be limited to:

4.4.3. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.

4.4.4. Threatening, intimidating or harassing other users, employees and students including any message that could constitute bullying or harassment, e.g. on the grounds of sex, race, disability, religion or belief, sexual orientation or age.

4.4.5. Using obscene, profane or abusive language.

4.4.6. Using language that could be calculated to incite hatred against any ethnic, religious or other minority group

4.4.7. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights

4.4.8. Defamation (genuine scholarly criticism is permitted)

4.4.9. Unsolicited advertising often referred to as “spamming”

4.4.10. Sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address

4.4.11. Attempts to break into or damage computer systems or data held thereon

4.4.12. Actions or inactions which intentionally or unintentionally cause a breach of the Oasis IT Security Policy including but not limited to:

4.4.13. Aiding the distribution of computer viruses or other malicious software.

4.4.14. Attempts to access or actions intended to facilitate access to computers, software and data for which the individual is not authorised

4.4.15. Using the network for unauthenticated access

4.4.16. The introduction or connection of unauthorised hardware to the Oasis IT Network infrastructure

4.4.17. Using the ICT facilities to conduct personal commercial business or trading

4.4.18. These restrictions should be taken to mean, for example, that the following activities will normally be a breach of policy:

4.4.19. Downloading, distribution, or storage of music, video, film or other material, for which you do not hold a valid licence or other valid permission form the copyright holder

4.4.20. Distribution or storage by any means of pirated software

4.4.21. Connecting an unauthorised device to the network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy

4.4.22. Circumvention of network access control

4.4.23. Monitoring or interception of network traffic, without permission

4.4.24. Probing for the security weaknesses of systems by methods such as port-scanning, without permission

4.4.25. Associating any device to Network Access Points, including wireless, to which users are not authorised

4.4.26. Non-Oasis related activities which generate heavy network traffic, especially those which interfere with others’ legitimate use of ICT services or which incur financial costs

4.4.27. Excessive use of resources such as file storage, leading to a denial of service to others, especially when compounded by not responding to requests for action

4.4.28. Frivolous use of ICT services, especially where such activities interfere with others’ legitimate use of ICT services

4.4.29. Use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.

4.4.30. Copying of other peoples’ website material without the express permission of the copyright holder

4.4.31. Use of peer-to-peer and related applications. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA

4.4.32. Software may not be copied, installed, or used on Oasis IT equipment except as permitted by the owner of the software and by law. Oasis IT services will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license

4.4.33. It is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software provided by Oasis IT Services may only be used as part of the user's duties as an employee or student for educational purposes.

4.4.34. The user must abide by all the licencing agreements for software entered into by Oasis with other parties, noting that the right to use any such software outside Oasis premises will cease when the individual leaves the organisation. Any software on a privately-owned computer that has been licensed under an Oasis agreement must then be removed from it, as well as ensuring the destruction of any Oasis owned data.

## 4.5. Exemptions from Unacceptable Use

4.5.1. There are a number of legitimate activities that may be carried out using Oasis IT systems that could be considered unacceptable use, as defined in this policy. This Section 5 of the policy defines exemptions from unacceptable use of Oasis IT Systems. However, for the absence of doubt clause 4.1 of this policy will apply in all circumstances and without exception.

4.5.2. Research involving defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material, obscene or indecent material or other unacceptable content including research into computer intrusion techniques is permitted only with the prior authorisation of an authorised Director of the Oasis Entity and the Director of Information Technology.

4.5.3. In such circumstances advice should be sought from Oasis IT Services and notification made by following procedure outlined in the Oasis Safeguarding Policy.

4.5.4. The Oasis IT Services team are required to undertake work, which from time to time may be considered a breach of this policy. For example, but not limited to, the setup systems/services, to test the security and other protections of the system, access to systems or services in the course of authorised duties, to test the limits of the systems performance or to reproduce the actions or potential actions of user. The Oasis IT Services team are exempt from the restrictions of this policy for Acceptable Use to the extent that the activities undertaken are required in the completion of their duties as authorised by the Director of Information Technology or other IT managers acting with delegated authority.

## 4.6. Consequences of breach of policy

4.6.1. Incidents of misuse will be dealt with by Oasis in accordance with the Behaviour for Learning Policy (students) or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff). The appropriate level of sanctions will be applied as determined by the nature of the identified misuse.

4.6.2. In the event of a breach of this Acceptable Use of Technology Policy by a user, Oasis may in its sole discretion:

4.6.2.1. restrict or terminate a user's right to use Oasis IT facilities;

4.6.2.2. withdraw or remove any material uploaded by that user in contravention of this Policy;

4.6.2.3. where appropriate, disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith;

## Appendix 1 – 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 |
| 4.1.1 & 4.1.4 Compliance with the Terms of Use of the IT System | | A | | | | | | | | | | C | C | C | C | C | C | C | C | C |
| 4.1.3 All Entities make use of the same Terms of Use | | | A | I | I | | R | R | | | | R | R | R | R | I | I | I | I | I |
| 4.1.5 Users required to accept Terms of Use where possible | | | | | | | | | | | | A | R | R | R | R | R | | | |
| 4.2.3 – 4.2.4 User Account Accountability | | A | | | | | | | | | | C | C | C | C | C | C | C | C | C |
| 4.3.1 – 4.3.4 Monitoring in accordance with the Device Monitoring Policy | | I | I | I | I | I | I | C | I | I | C | A | R | R | R | R | R | R | R | R |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.4.1 – 4.4.6 Unacceptable Use | | A | | | | | | | | | | C | C | C | C | C | C | C | C | C |
| 4.5.1 Unacceptable Use | | A | | | | | | | | | | C | C | C | C | C | C | C | C | C |
| 4.5.2 – 4.5.3 Exemptions from Unacceptable use – Legitimate Research | | A | | C | C | | C | C | | C | | C | | | | | | | | |
| 4.5.4 Exemptions from Unacceptable use – IT Duties | | | | | | | | | | | | A | R | R | R | R | R | R | R | R |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | |

## Appendix 2 – Terms of Use of Oasis IT Systems

These are the Terms and Conditions for the Acceptable Use Agreement 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 E-Safety 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 with 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 not install or attempt to install programmes of any type on a device, or store programmes on a device, nor will I try to alter computer settings, unless allowed within my Oasis role and level of permissions.
- ✓ I will not disable or cause any damage to Oasis equipment, or equipment belonging to others.
- ✓ 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 |
|---|---|---|---|---|
| 0.6 | September 2017 | Amended by IT Project Consultant, Liz Hankin | IT Policy Working Group | Updated to reflect Policy for all OCT users/staff |
| 0.6.2 | October 2017 | Amended by IT Project Consultant, Liz Hankin | IT Policy Working Group | Updated post review meeting 02/10 |
| 0.6.7 | 20/12/2017 | Amended by IT Project Consultant, Liz Hankin | IT Policy Working Group | Draft version for editing by Rob Lamont |
| 1.0 | 28-12-17 | Amended by Director of Information Technology, Rob Lamont | Chief Operating Officer, John Barneby and Dave Parr, CEO of OCP and OCT. | Final Draft for Approval |
| 1.1 | 11-6-18 | Amended by Data Protection Officer, Sarah Otto | OCL | DPO review |
| 1.2 | 01-04-19 | Amended by Director of Information Technology, Rob Lamont | Regional Director for the Midlands, Paul Tarry | Reviewed and Updated |
| 1.3 | 23-05-2019 | Owned and Amended by IT Business Relationship Manager, Marc Hundley | Director of Information Technology, Rob Lamont | Reviewed and Updated |

**Policy Tier**

☐ Tier 1

☒ Tier 2

☐ Tier 3

☐ Tier 4

**Owner**

IT Business Relationship Manager

**Contact in case of query**

Marc.hundley@oasisuk.org

## Approvals

This document requires the following approvals.

| Name | Position | Date Approved | Version |
|---|---|---|---|
| John Barneby | Chief Operating Officer | July 2019 | V1.3 |
| | | | |
| | | | |
| | | | |

## 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 |
|---|---|---|---|
| Available to all staff | Policy portal | 24 July 2019 | V1.3 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |