ACCEPTABLE USE OF TECHNOLOGIES

Acceptable Use of Technologies Policy
V4.0
Mark Thornton / April 2023

CONTENTS

At a glance

OCL is part of the wider Oasis family with a shared vision for community, a place where everyone is included, making a contribution and reaching their God-given potential. This policy has been drawn up in accordance with the Oasis Ethos and 9 Habits.

With this in mind, we acknowledge that 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. 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 technologies needs to be undertaken in a way that maximises the benefits, ensures that the infrastructure is not abused and is available to use.

Checklist

- ❑ We all use Oasis IT systems and equipment on the basis that we accept and agree to follow the contents of this policy, on acceptable use of Oasis technologies.
- ❑ We all need to know what Oasis Acceptable Use of Technologies Policy (AUTP) means to us as users of Oasis systems. This policy will be used for our personal development through training provided by Oasis.
- ❑ We are all responsible for what we do on the Oasis systems and need stay safe while using the internet and other communications technologies for educational, personal and recreational use. Oasis IT Services will ensure that there is a safe system in place for all users.
- ❑ We will all ensure that our use of Oasis IT systems protects Oasis IT systems and other users from accidental or deliberate misuse that could put the security of the systems and other users at risk.
- ❑ We will ensure that any new staff and students will receive guidance on this policy as part of their induction process.

In brief

The policy has been developed to allow all 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 that all users are confident in using the Oasis IT technologies, this policy sets out the requirements, responsibilities and accountabilities associated for use of Oasis IT Services managed network resources. This includes the use of any online Oasis systems such as Microsoft Office 365, the internet, e-mail, instant messaging, social media, media publications, file transmission and online 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 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 Acceptable Use of Technologies Policy (AUTP).

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 through accepting the relevant online Acceptable Use Agreement.

Terms of use of Oasis IT systems and equipment

By accessing the Oasis IT systems and resources, all users agree to adhere to the 'Terms of Use of the Oasis IT System' as found in Appendix 2. Failure to adhere to these 'Terms of Use' is a breach of this policy.

Where possible, users will be required to accept the 'Terms of Use' when accessing the system through the Acceptable Use Agreement as documented in Appendix 2. As a result of technical limitation of some systems, this will not always be displayed. Users accessing the system are deemed to have accepted the Terms of Use regardless of whether they are displayed prior to logon or not.

All users will adhere to the Oasis E-Safety Policy, Oasis Password Policy and guidelines, Oasis Data Protection Policy, Oasis Information Security Policy and OCL Safeguarding and Child Protection Policy, in addition to all relevant regulatory and legal requirements as relevant to their account permissions. Appendix 1 contains a list of all related OCL Policies.

Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken. An investigation will include but will not be limited to appropriate audit logs, backups, retained data.

Monitoring use of Oasis IT systems

OCL expects all users to treat colleagues, students, parents, volunteers, contractors, visitors and members of the public with dignity and respect, and in line with the Oasis Ethos and 9 Habits.

With this in mind, 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 networks, systems and equipment, including anything created, stored, sent or received through the Oasis Cloud system on a personal device.

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 E-Safety Policy, Oasis Device Monitoring Policy and the Oasis Web Filtering Policy, which are available through the Policy Portal and specific requirements and responsibilities are outlined in Appendix 1.

Unacceptable use of the Oasis IT systems

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

Specific unacceptable use of the Oasis IT System may include but is not limited to:

- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
- 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, marriage and civil partnership, religion or belief, sexual orientation, gender reassignment, pregnancy or maternity.
- Inappropriate conduct and social media presence, as defined in the latest version currently in force of "Keeping Children Safe in Education".
- Using obscene, profane or abusive language.
- Using language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral right.
- Disclosing personal username or passwords.
- Using or attempting to use another person's username and password.

- Defamation (genuine scholarly criticism is permitted).
- Unsolicited advertising often referred to as “spamming”.
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address.
- Attempts to access, download, edit or redistribute information or damage computer systems where information is located.

Actions or inactions which intentionally or unintentionally cause a breach of the Oasis IT Security Policy

Actions or inactions which intentionally or unintentionally include a breach of the IT Security Policy include but are not limited to:

- Aiding the distribution of computer viruses or other malicious software.
- Attempts to access or actions intended to facilitate access to computers, software and data for which the individual is not authorised.
- Using the network for unauthenticated access.
- The introduction or connection of unauthorised hardware to the Oasis IT Network infrastructure.
- Using the systems for anything that is not Oasis related i.e. for personal use or for business activities that are not Oasis.

Activities normally in breach of policy

The activities that normally breach the requirements of OCL policy are:

- Downloading, distributing or storing music, video, film or other material, for which you do not hold a valid licence or other valid permission form the copyright holder.
- Distribution or storage by any means of pirated software.
- 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.
- Circumvention of network access control.
- Monitoring or interception of network traffic, without permission.
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission.
- Associating any device to Network Access Points, including wireless, to which users are not authorised.
- 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.
- 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.
- Frivolous use of ICT services, especially where such activities interfere with others’ legitimate use of ICT services.

- Use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.
- Copying of other peoples' website material without the express permission of the copyright holder.
- Use of peer-to-peer and related applications. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA, 'Cryptomining'.

Use of Oasis licensed software

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 licence.

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.

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 when the individual leaves the organisation.

Use of Oasis data

When an individual leaves the organisation they must ensure the destruction of any Oasis owned data from any privately owned devices that have been used whilst a member of the organisation.

Any use of Oasis data on a personal device and privately owned devices must comply with the Oasis Information Security Policy.

Exemptions for unacceptable use

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. The following are recognised as exemptions from unacceptable use of Oasis IT Systems.

The exemptions are as follows:

- 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.

- In such circumstances advice should be sought from Oasis IT Services and notification made by following procedure outlined in the Oasis Safeguarding Policy.
- 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 the 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.
- Exemption due to specific requests for information with legal or statutory requirements.

Consequences of a breach of AUTP

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.

In the event of a breach of this AUTP by a user, Oasis may in its sole discretion:

- restrict or terminate a user's right to use Oasis IT facilities.
- withdraw or remove any material uploaded by that user in contravention of this Policy.

Training Requirements

As part of the personal development of all users of Oasis IT systems, Oasis has provided training materials that cover the key areas of safe and responsible use of the systems. These materials will be available for academy-led scheduled sessions throughout the academic year.

Training sessions will provide every user with an up-to-date knowledge for the use of the Oasis IT systems. Training sessions will either be academy-led and directed sessions or scheduled sessions as part of the national training days.

Oasis student users and their parents should have access to the relevant Terms of Use of Oasis IT systems and equipment document as outlined in the Acceptable Use Agreement Appendix 2. These documents will be as part of a training package for

academies to use within their own programmes informing users of their personal responsibility and what Oasis will be doing to maintain their safety.

Statutory requirements

- Copyright, Designs and Patents Act 1988
- Communications Act 2003
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Trademarks 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
- The PREVENT Duty Guidance

Oasis staff, agency and volunteers 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 and the Oasis Information Security Policies.

Please refer to Appendix 1 for details of all current Oasis Policies, standards and processes that users should be aware of and read in conjunction with this AUTP.

Keeping Children Safe in Education

The Department for Education (DfE) has provided statutory guidance for all schools to implement. The information below has been taken from an Annex in the document and has relevance to how the DfE guidance defines and requires schools to behave with regard to Cybercrime.

'This is statutory guidance from the Department for Education ('the Department') issued under Section 175 of the Education Act 2002 (as amended), the Education (Independent School Standards) Regulations 2014, the Non-Maintained Special Schools (England) Regulations 2015 and the Apprenticeships, Skills, Children and Learning Act 2009 (as amended). Schools and colleges in England ***must*** *have regard to it when carrying out their duties to safeguard and promote the welfare of children. For the purposes of this guidance children includes everyone under the age of 18. Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are*

enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).
Cyber-dependent crimes include:

- *unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded.*
- *'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,*
- *making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.*

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.
Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.'

Additional advice can be found at:

- Cyber Choices
- When to call the police
- National Cybersecurity Centre - NCSC.gov.uk

RACI Matrix

Policy Element	Leadership & National									Academy				IT Directorate					
	Board	OCL CEO	OCL COO	OCL Deputy COO	National Director of Academies	National Director of Communications	Regional Directors & Service Directors	Head of Compliance	Data Protection Officer	Academy Principal & ALT, Safeguard Lead, Data Protection Lead	Academy Staff	Academy Students	Parents / Carers	Director Information Technology	National Infrastructure Manager	Heads of IT Security & National Projects	IT Service Desk Manager & Support Technicians	Head of Information	IT Cluster Managers & Cluster Technicians
We accept and agree to follow the contents of this policy, on acceptable use of Oasis technologies.	I	I	I	I	I	I	C	C	C	A	R	R	R	A	C	C	I	C	I
This policy will be used for personal development through training provided by Oasis.	I	I	I	I	C	C	C	I	I	A	R	R		C	I	I	I	I	I
We are all responsible for our use of Oasis systems	I	I	I	I	I	I	I	I	I	R	R	R	I	C	I	I	I	C	I

for educational, personal and recreational use.																			
Oasis IT Services will ensure that there is a safe system in place for all users.	I	I	I	I	I	C	C	I	I	I	I	I	I	R	R	R	A	C	A
We will all ensure that our use of Oasis IT systems protects the systems and other users from accidental or deliberate misuse.	I	I	I	I	I	I	C	I	C	A	R	R		A	C	C	C	I	I
We will ensure that any new staff and students will receive guidance on this policy as part of their induction process.	I	I	I	I	I	C	I	C	A	R	I	I	I	C	I	I	I	I	I

APPENDIX 1 – Related Oasis Policies, Standards, Processes and Resources

Oasis Policies and resources

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

- OCL Safeguarding and Child Protection Policy
- The Oasis Device Monitoring Policy
- The Oasis Web Filtering Policy
- The Oasis Data Protection Policy
- Use of Email Policy
- E-Safety Policy
- The Oasis Online Safety Curriculum Policy
- The Oasis IT Access Policy
- The Oasis IT Security Policy
- The Oasis Information Security Policy
- Use of Personally Owned Devices Policy
- Data Retention Policy
- Password Policy

Related documents and SharePoint resources

- Guide to Horizon's Operational Best Practice for Oasis Academies
- Cybersecurity resources – staff and students
- Oasis Online Safety Curriculum

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 E-Safety 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 to support this:
✓ When I use personally owned devices (e.g. handheld / 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.

Student Acceptable Use of Technologies Agreements

- Parents/Carers are provided with access to Acceptable User Agreement that their child will be expected to agree to prior to gaining access to the Oasis IT Systems.

- The parent/carer's wish to allow their child to attend and be educated within an Oasis Academy where the use of IT systems is integral to the teaching and learning is seen as agreeing to their child's use of the Oasis IT systems, including the Internet and email.

- Parents/Carers are required to explicitly choose to 'Opt-out' should they not agree with this principle.

Oasis Horizons devices – Home Use Agreements

Every Oasis user who is issued within Oasis Horizons iPad is required to sign an agreement that specifically addresses the issues relating to their use of the iPad.

There are two agreements:

- Home Use Agreement for parents/carers or student's signature.
- Home Use Agreement for Oasis Staff.

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
2.0	14-11-2022	Owned by Director Information Technology, Mark Thornton, amended by Liz Hankin	Director Information Technology, Mark Thornton, Sarah Graham	Reviewed for Sept KCSIE and edited update to OCL Policy Template
3.0	20-03-2023	Owned by Director Information Technology, Mark Thornton, amended by Liz Hankin	Director Information Technology, Mark Thornton, Sarah Graham	Reviewed and edited post review by IT Directorate
4.0	26-04-2023	Owned by Director Information Technology, Mark Thornton, amended by Liz Hankin	Director Information Technology, Mark Thornton, IT Service Managers	Reviewed and edited post review by Sarah Graham and IT Directorate

Policy Tier

☐ Tier 1
☒ Tier 2
☐ Tier 3
☐ Tier 4

Owner

Mark Thornton, OCL Director Information Technology

Contact in case of query

Mark Thornton, OCL Director Information Technology, mark.thornton@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
Approval not required as policy reviewed	N/A	N/A	N/A

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
Not applicable / Insert

Location
Tick all that apply:
☐ OCL website
☐ Academy website
☒ Policy portal
☐ Other: state

Customisation
☒ OCL policy
☐ OCL 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 OCL staff	Policy Portal	30/8/23	V4.0