E-SAFETY POLICY

April 2021

CONTENTS

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

1.1 This policy gives clear guidance about the Oasis approach to E-Safety. The purpose of this policy is to provide details of personal responsibilities and accountability for use of Oasis IT systems and devices.

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

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

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

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

1.5 Therefore, right at the heart of Oasis is this deep-rooted commitment to inclusion, equality, good relationships, hope and perseverance. This is inescapable and must be core to our delivery of this E Safety policy. We are committed to providing a safe environment for all our students so they can learn in a relaxed, secure atmosphere and have every opportunity to thrive and become the very best version of themselves.

The Oasis 9 Habits

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

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

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

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

All of this is detailed in our Education Charter.

Introduction

1.9 Fundamentally, we are clear that E safety is a safeguarding responsibility. It is the policy of Oasis Community Learning (OCL) to protect users from harm, so far as is reasonably practicable, whilst maximising the educational and social benefits of using technology.

1.10 OCL will take reasonable steps to ensure that all users of technology can be safe online whilst recognising that developing a responsible attitude to E-Safety through education is key to ensuring that young people are able to flourish in a world that increasingly requires and promotes digital fluency and engagement. The intention being, when young people make use of technology that is new to them, they will act in a responsible and safe way.

1.11 The policy has been developed to allow OCL to fulfil our obligations to safeguarding staff, the young and vulnerable people within our care, wider legal responsibilities and the need to effectively manage the IT services whilst respecting and maintaining the privacy of users.

1.12 The contents of this document are fully compliant with the DfE statutory guidelines 'Keeping Children Safe in Education (KCSiE) 2020' and will be reviewed after the Government's 2021 consultation stage has been completed and place the DSL with responsibility of e-safety within an Academy. The legal requirements of the KCSiE guidelines are consistent with those designated as mandatory within this document. There is a requirement within the KCSIE document for schools and colleges to ensure that all authorised staff users to receive regular E-Safety and Online Safety training. This policy should be used in conjunction with the Oasis Online Safety Policy, the Oasis Online Safety Curriculum Policy and the Oasis Horizons 1:1 Device Policy.

1.13 OCL 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. This policy is designed to help Oasis academies to be compliant with this statutory duty.

1.14 This policy will be amended on a regular basis to take into account changes in best practice, legislation and wider Oasis policy.

2. What is this policy about?

In brief

2.1 Technology and use of the internet is the reality of modern life. This policy sets out how OCL will go about both protecting and supporting the young people in making use of technology in a safe manner within the context of OCL's wider safeguarding policies and practices

2.2 It sets out both the technical and organisational requirements to minimise the likelihood of all users including young people and vulnerable individuals being exposed to inappropriate material and being placed at risk through inappropriate interactions or contact including the

restrictions, filtering and monitoring that should be put in place along with the process of providing education and information to ensure users are appropriately informed.

In more detail

2.3 OCL acknowledges that technology can improve the planning, managing workload and delivery of teaching as well as making the learning experience more dynamic and interactive for students. Therefore, OCL will support the best accountable practice for embedding effective use of technology in teaching and learning across all Oasis activities.

2.4 OCL recognises that all professionals need to use technology to enhance their working practice and develop innovative ways of personalising learning to suit the different aptitudes and interests of learners, including those with special needs.

2.5 Whilst technical solutions must be put in place to ensure that users are not exposed to risk, it is also key to prepare young people to be safe and responsible users of technology in the world outside of the protections provided within the Oasis IT System.

2.6 All academies must follow and deliver the Oasis Online Safety Curriculum Policy, this, in conjunction with other online safety tools provided by OCL, provides a reliable source of tuition and practical tips to keep users safe with up-to-date information. The specific policies that have direct relevance to this policy are listed in Section 5 of this policy.

3. Who is this policy for?

3.1 This policy applies to the following Oasis Entities:

- Oasis Community Learning (OCL) including all Oasis Academies
- Oasis IT Services Ltd

3.2 This E-Safety Policy applies without exception to all users of ICT facilities and equipment owned by OCL including access to services provided via personally owned equipment. This includes staff, students and any visitors who have been provided with temporary access privileges.

3.3 This policy and procedure will be maintained in in line with the current published version of the Keeping Children Safe in Education DfE statutory guidance and is designed to ensure that this guidance is enacted in all applicable contexts.

4. The requirements that apply to this policy

4.1 This Oasis E-Safety Policy requires integration with the following Oasis Policies:

- OCL Safeguarding and Child Protection Policy
- OCL Anti-bullying Policy
- OCL Behaviour for Learning Policy
- OCL Curriculum Policy (Primary)
- OCL Teaching and learning Policy & Guidance (Primary)
- OCL Curriculum Policy (Secondary)
- OCL Teaching and Learning Policy (Secondary)

- OCL Parental/Carer's Code of Conduct Policy
- OCL Offsite activities and educational visits Policy
- The Oasis Horizons 1:1 Device Policy
- The Oasis Online Safety Curriculum Policy
- The Oasis Data Protection Policy
- The Oasis Password Policy
- The Oasis use of Email Policy
- The Oasis Acceptable Use of Technologies Policy
- The Oasis Information Security Policy
- The Oasis Web Filtering Policy

Applicable legislation

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

- Copyright, Designs and Patents Act 1988 (legislation.gov.uk)
- Malicious Communications Act 1988 (legislation.gov.uk)
- Computer Misuse Act 1990 (legislation.gov.uk)
- Criminal Justice and Public Order Act 1994 (legislation.gov.uk)
- Trade Marks Act 1994 (legislation.gov.uk)
- Data protection – GOV.UK (www.gov.uk)
- Human Rights Act 1998 (legislation.gov.uk)
- Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)
- Freedom of Information Act 2000 (legislation.gov.uk)
- Communications Act 2003 (legislation.gov.uk)
- Criminal Justice and Immigration Act 2008 (legislation.gov.uk)
- Keeping children safe in education (2020) – GOV.UK (www.gov.uk)
- Guide to General Data protection Regulation – GOV.UK (www.gov.uk)
- Prevent review (publishing.service.gov.uk)

5. Policy Scope

5.1 This policy applies to activities in any location where access to and the use of any Oasis ICT systems and/or equipment takes place, e.g., Oasis Horizons devices at home; remote access to any online Oasis system; Microsoft Office 365; networked resources within the academy.

5.2 The policy includes the use of personally owned devices both within and outside of Oasis premises when being used to access Oasis provided IT Services.

5.3 To make use of IT facilities provided by Oasis, 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.

5.4 The Oasis Online Safety Curriculum Guidance Notes contain full details of age specific content that must be delivered to comply with this E-Safety Policy. This document is frequently updated

to ensure compliance with published legal requirements and is available for all staff on OasisZone.

6. Academy application of and compliance to E-Safety Policy

6.1 This policy recognises that effective E-Safety in an educational setting is met through a combination of appropriate technology controls to limit and monitor access and comprehensive and age-appropriate education for young people.

6.2 Oasis Horizons extends the use of OCL owned devices by students beyond the confines of Oasis sites and the Oasis Network. It means that the educating young people and their parents in relation to online safety and the safe use of technology becomes increasingly important due to the reduction in supervision and technical controls which are possible when devices are used away from an Oasis Academy.

6.3 E-Safety is intrinsically linked to IT Security and therefore adherence to the IT Security Policy is critical at all times.

6.4 To support compliance with this policy, an academy must ensure that all students actively supported in the development of the skills and knowledge to remain safe whilst using technology and when online. The Online Safety Curriculum Policy is provided to support this process and includes resources to educate young people in the safe use of technology.

6.5 Oasis will ensure that parents are effectively supported in with advice about E-Safety risks and how best to deal with them through the deployment of the 'Safer Schools App' and through resources posted on academy websites.

7. Roles and Responsibilities

7.1 Individual users are responsible for making sure that they understand what their role and the responsibility it entails.

7.2 Individual users are required to agree to this Oasis E-Safety Policy when they access Oasis IT Systems or devices. Where technically possible, when accessing the system for the first time, users will need to agree to the acceptable use of the IT System.

7.3 Oasis IT Services is responsible for ensuring that all reasonable and appropriate steps have been taken to protect users whilst using Information Technology. This involves ensuring appropriate technology is in place to protect users from accessing inappropriate material.

7.4 Oasis will take every opportunity to help staff, students and their parents/carers understand E-Safety issues through staff training, parents' meetings, newsletters, letters, website, online Apps and learning spaces as well as providing information about national and local E- Safety campaigns, for example Safe Internet Days.

7.5 Academies must ensure that they are enrolled for use of the 'Safer Schools App' and that its use has been actively promoted to parents and students.

7.6 Acceptable User Agreements form the agreement between any authorised user of Oasis IT systems and Oasis. Oasis have a standard Acceptable Use of Technologies Policy which applies to all users of the system. Academies must ensure that the Acceptable Use of

Technologies Policy is explained, issued and signed by the different users of the Oasis system and equipment.

7.7 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.

7.8 Academies must put in place processes to detail how any breaches of the E-Safety Policy will be documented, reported and dealt with.

8. E-Safety and the Oasis Horizons Project

8.1 Oasis Horizons is an exciting programme to ensure that all young people within OCL have equality of access to technology and can benefit from its capabilities to ensure that they are able to fulfil their potential. However, the deployment of OCL devices for use by students beyond the academy does need to be carefully considered in the application of E-Safety best practice.

8.2 Horizons Devices will only be issued after the completion of a signed parental agreement. The management and deployment of Oasis Horizons Devices is controlled by the Oasis Horizons Policy.

8.3 Whilst OCL must take what steps it can to limit the E-Safety risks associated with the deployment of Oasis Horizons, it is recognised that the technological capabilities to restrict and monitor the activity of students on these devices when away from the academy is more limited than when they are on an academy site.

8.4 OCL will ensure that Parents/Carers are provided with appropriate information and support to enable them to manage the risks associated with young people making use of technology when away from the academy including the use of Oasis Horizons devices.

8.5 Oasis IT Services have made the 'Jamf' Parents App is available which allows parents to implement some technical controls over the use of the Horizons device when it is away from the academy in line with their wishes.

9. Internet Access, Monitoring and Filtering

9.1 OCL reserves the right to monitor the use of all Oasis IT Services including email, telephone and any other electronic communications, whether stored or in transit, in line with relevant legislation. All monitoring will be carried out in compliance with the Oasis Device Monitoring Policy.

9.2 All Oasis Users provided with an Oasis Horizons device will have access to the internet and social media according to the Oasis Horizons 1:1 Device Policy. This includes all monitoring and filtering.

9.3 OCL makes use of a monitoring solution (Smoothwall Moderated Monitor) installed on all student and academy-based staff Microsoft Windows devices. This software will be installed, configured

and managed as the Oasis Device Monitoring Policy. This software is used to monitor activities undertaken on the devices and alert the academy to any safeguarding concerns. The provider monitors and categorises incidents of safeguarding concern for the attention of the academy.

9.4 Academy DSLs are responsible for administering and monitoring this system and responding to alerts from the provider. Regular automated reports are provided to DSLs who must ensure that these reports are checked and that any alerts are investigated, and appropriate action is taken.

9.5 Oasis implement network level filtering within the Oasis Network (Smoothwall Filter) to help to control and prevent access to inappropriate and other undesirable information on the internet. The implementation of the filtering will be carried out in accordance with the Oasis Web Filtering Policy and changes to filtering rules will be made as per the Oasis Web Filtering Changes Process.

9.6 Network level filters can be modified, in accordance with Oasis Web Filtering policy on an academy-by-academy basis. Network level filters are applied to the individual and as such can be tailored to role and age specific requirements.

9.7 Reports are provided to Academy DSLs highlighting activities which have been blocked by the network level filters but that could indicate an issue of concern. For example, highlighting a student searching for inappropriate or harmful content. Academy DSLs are responsible for monitoring these reports and following up any issues of concern.

9.8 It should be noted that devices which are accessing the internet through a ¾/5G connection, including oasis devices within a physical oasis location are outside of the Oasis network and therefore not subject network level filtering.

9.9 Academy devices which are used to access the internet away from the Oasis Network, including but not limited to Oasis Horizons iPads, are deployed with a filtering solution (Cisco Umbrella). This filtering solution will apply whenever a device connects to the internet outside of the Oasis Network e.g. from home internet connections.

9.10 Offsite filtering is applied uniformly to all academies. Different filtering can be applied to primary and secondary students and for staff.

9.11 Oasis IT Services provide a dashboard for Academy DSLs which highlights blocked activity carried out on a device when it is used.

9.12 Oasis IT Services will implement ‘Safe Search’ where possible. Safe Search indicates to supported search engines that inappropriate content should be removed from the search results. The interpretation of inappropriate content is provided by the search engine themselves and it is not supported by all search engine providers.

9.13 The Oasis filtering software solutions will help to prevent access to inappropriate sites available over the internet. However, no automatic filtering service can be 100% effective in preventing access to such sites and it is possible that users may accidentally access unsavoury material whilst using the internet. In such circumstances, users must exit the site immediately and advise DSL, providing details of the site, including the web address, to reduce the possibility of the material being accessed again in future. Details of the inappropriate material accessed must be logged with Oasis IT Services via the IT Services Desk (ServiceDesk@Oasisuk.org). The Oasis IT Services team will arrange for the filtering rules to be examined to block future access to the site in accordance with Oasis Web Filtering Policy and Oasis Web Filtering Changes Process.

9.14 Domestic Internet Service Providers provide filtering solutions as part of the internet access service they provide. It is recommended that all users implement these filters to provide protection for young people when using the internet when away from the Oasis Network.

10. Unacceptable use of computers, mobile devices (including phones) and network resources

10.1 All users must make themselves aware of the Oasis Acceptable Use of Technologies Policy for the processes and good practices required to retain access to the Oasis IT systems.

10.2 Staff and students should consider the spirit of the Oasis Ethos when working on Oasis IT systems. Any conduct which may discredit or harm OCL, its reputation, its staff or the IT facilities or can otherwise be considered intentionally unethical (including but not limited to; cyber bullying, sexual harassment or threatening behaviours) is deemed unacceptable.

10.3 Staff and students should consider the spirit of the Oasis Ethos when using public IT Services such as, but not limited to social media, in a personal capacity. Any conduct which may discredit or harm OCL, its reputation, its staff or the IT facilities or can otherwise be considered intentionally unethical is deemed unacceptable. Any conduct which undermines a staff members ability to fulfil their role within the organisation including but not limited to their standing and reputation within the community is deemed unacceptable. (including but not limited to, cyber bullying, sexual harassment or threatening behaviours)

10.4 Incidents of unacceptable conduct 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 reported misuse.

10.5 Where an Academy chooses to permit student mobile phones and mobile devices within the Academy there must be a clear statement for the permitted use, restrictions and sanctions that are permitted within the Academy.

11. Student Accounts and Passwords

11.1 The security and integrity of a staff member and student's account is essential for the safety of the user and the other users of the Oasis IT System

11.2 Each staff member and student will have their own, individual 'OasisNet' account which is used to access Oasis IT Systems. Access will be granted based on the role of the individual to ensure that they are only able to access information that is suitable for them. Therefore, account information must not be shared. This includes logging others onto an Oasis device using another individual's account.

11.3 Passwords will be applied as per the Oasis Password Policy.

11.4 The use of shared accounts or class accounts is not permitted for students who are in year one or higher.

11.5 Should a user believe their password has been compromised, they must immediately report this to Oasis IT Services either by informing an adult at the academy or by submitting a support

request by emailing servicedesk@oasisuk.org. The account will, according to context of the breach, either have the password reset or will be deactivated to protect the account while further investigation is carried out.

11.6 Users are responsible and accountable for maintaining the security of their personal password and must take all reasonable steps to keep their passwords confidential and must not disclose them to anyone else.

11.7 OCL maintains the right to access the unique Oasis account and associated resources of staff members and students after termination of employment or attendance at an academy for operational reasons and for the continuing delivery of services as stated in the Oasis Access Policy and Oasis Deletion of Accounts Policy.

12. Email

12.1 The Oasis organisation-wide email system provides, where appropriate, staff and students with a unique Oasis account for their individual use. Access to this email account will be rescinded on termination of employment or attendance at an Academy and all other network access revoked in accordance with the Oasis User Deletion Policy.

12.2 However, un-regulated email can provide a means of access that bypasses the traditional Academy boundaries, and it is difficult to control content. Therefore, in Oasis context, email is not considered private. Oasis reserves the right to monitor email accounts. To maintain the safety of staff and students, it is the policy of Oasis to filter incoming and outgoing emails for viruses and potentially harmful attachments.

12.3 All authorised users must comply with the Oasis Use of Email Policy.

12.4 Oasis realise that any filtering is not 100% effective, and there is a clear commitment to educate staff and students to become responsible users of email and to be accountable for their personal use by becoming self-regulating to a large extent.

12.5 If an offensive email is received by any user, the Oasis IT Services Desk team or a person responsible for ICT within the Academy must be contacted immediately so that appropriate measures can be taken.

12.6 Students who choose to misuse the email system will be subject to disciplinary procedures as outlined in the Behaviour for Learning Policy.

12.7 Staff who choose to misuse the email system may be subject to disciplinary procedures.

12.8 The email system is provided to support and facilitate the work carried out by a user whilst they are part of the Oasis family. The email system should not be used for personal correspondence or messaging.

12.9 Personal email or messaging between staff and students is forbidden.

12.10 Students in Year 3 or below will not be able to send individual emails from their Oasis User accounts. For students in Year 4 and Year 5 rules are in place restricting to internal mail flow only. They will not be able to email external addresses. A Student in Year 6 or above has no mail flow restrictions – student can send and receive email internally and externally.

13. Publication of Personal Data

13.1 The management of all personal data relating to staff and students must be conducted in accordance with the Oasis Data Protection Policy.

13.2 Care must be taken when capturing images or videos to ensure that all individuals are appropriately dressed and explicit written permission for use has been gained from parents and carers/the individual in line with the Data Protection Policy. This may be altered or amended at any time by the parent or carer or by the student themselves.

14. Video Conferencing, Chat & Instant Messaging

14.1 Students will be allowed to use Oasis IT Services Managed Video Conferencing/online meeting functionality within a controlled educational context under the guidance of Oasis staff who are responsible and accountable for ensuring and verifying the authenticity of all participants.

14.2 Oasis makes use of Microsoft Teams as part of Microsoft Office 365. This enables staff, teachers, students and parents/carers to jointly celebrate, share and learn from one another. The delivery of remote learning is a powerful way of continuing education when students are away from the classroom.

14.3 The use of 'cameras' as part of the delivery of online and remote learning is encourage as it allows a teacher to actively monitor participation and engagement in the lesson. However, it is important to recognise that the use of cameras potentially provides a view into the personal lives of individuals and therefore care must be exercised.

14.4 It is important that staff and students understand that the delivery of learning or other forms of interaction via a video conference is no different to other forms of interaction that may happen in the course of their involvement with OCL. Therefore, the same standards of conduct, behaviour and etiquette are required during online interactions as would be expected in person. Staff should set clear expectations for students around the behaviour expected on video conferencing services and misbehaviour should be managed in line with OCL behaviour for learning policy.

14.5 Video Conferences/online meetings must include a member of staff who is responsible for moderating the behaviour and conduct of all participants.

14.6 Leaders must ensure that all staff leading video conference/online meeting sessions have been appropriately trained in the appropriate use of the technology and the controls to effectively moderate the meetings and safeguard participants from in appropriate activity.

14.7 Oasis IT Services will provide a range of training materials that can be used to support training in the best practice of video conference/online meeting tools.

14.8 Oasis IT Services can retrieve chat/instant message conversations undertaken using the Microsoft Office 365 environment.

14.9 Staff must record video conference interactions with students to ensure that it is possible verify what has happened in a given situation should the need arise.

14.10 The use of other chat / instant messaging / video conferencing tools within the Oasis network is prohibited except where there is a specific requirement to support interactions with a third party

using their system or to support a specific training need. Wider access to these tools will not be allowed by Oasis IT Services without a written instruction from the Chief Executive Officer.

15. Social Media

15.1 Social Media is a powerful influence on the society, a significant part of the social lives of many people and a critical method of communication and interaction.

15.2 Social Media takes many forms, but the content is largely unregulated and has the potential to expose young people to large amounts of inappropriate content. For the purposes of this policy, video sharing sites such as YouTube and Blogging sites are considered separately from other forms of Social Media.

15.3 This policy acknowledges the reality is that young people are routinely making use of Social Media and therefore it is vitally important that young people are supported in their understanding of how to stay safe in its use and their interactions online. The tools provided within the Oasis IT system provide a secure way of introducing students to the world of social networking and how to protect themselves as they become autonomous users of technology systems that fall outside of controlled school environment.

15.4 Social Media sites are routinely blocked for use within the Oasis IT Network as they have the potential to offer a distraction from the core purpose of the use of Technology in an academy and have the potential to present a E-Safety risk. However, it is recognised that some individuals may need access to Social Media in the course of their work and therefore access to social media may be granted at the discretion of the academy principal.

15.5 Oasis Devices including Horizons devices are restricted from accessing social media sites where the device is used away from the Oasis IT Network and the device is allocated to a student in the primary phase of education. Students in the secondary phase of education and staff are not restricted from accessing social media from Oasis devices when away from the Oasis Network.

15.6 Academies are encouraged to operate official social media channels to communicate with the wider academy community.

15.7 Public Social Media sites must not be used as part of teaching and learning or educational activity and students must not be directed to or required to participate in any social media service to be able to access or be informed of any of the services offered by an academy.

15.8 It is recognised that staff may wish to make use of Social Media in their personal lives. Staff are advised to consider carefully the implications of the publication of personal information on the internet and ramifications of being available within their professional lives. The publication of information relating to OCL in any way including details of employment may only be shared with the explicit permission of the line manager. Any publication of materials in a personal capacity must be explicitly identified as such.

15.9 Staff must not use social media as a method of communication with students and must not link or ‘Friend’ students to their personal social media channels.

16. Video Sharing Sites

16.1 It is recognised that Video Sharing sites often contain useful educational material / content that supports the effective delivery of teaching and learning. However, video sharing sites are unregulated and can contain inappropriate content.

16.2 Filtering of video content is technically challenging if access to a video sharing site is allowed and therefore access to video sharing sites presents some risks of students access inappropriate content which need to be weighed against the potential benefits. The decision to allow access to video sharing sites within the oasis network in an Oasis Academy resides with the Academy Principal.

16.3 It is recognised that staff may wish to publicly share videos in a personal capacity using video sharing sites. Staff are advised to consider carefully the implications of the publication of personal information on the internet and ramifications of this being available within their professional lives. The publication of information relating to OCL in any way including details of employment may only be shared with the explicit permission of the line manager. Any publication of materials in a personal capacity must be explicitly identified as such.

17. Blogs

17.1 It is relatively straight forward for an individual to create a personal blog which in turns allows them to post largely unregulated content on the internet for public consumption. Blogs are often hosted within common, public, blog hosting services. Blog platforms often include the ability to leave comments and feedback and to discuss to content. This discussion is often unmoderated.

17.2 Access to these services is managed through the Oasis Web Filtering Policy and the Oasis Web Filtering Change Process. However, it is possible and relatively straight forward for individuals to setup personal blogs away from common blog hosting services which may not be subject to these filtering rules. Where this is the case and the content are deemed to be inappropriate then the IT Service Desk should be notified immediately so that access can be restricted.

17.3 It is recognised that Blogs provide an opportunity for students to share and publish information as part of their educational activities. The use of Blogs by students as part of their education must take place on a platform managed and controlled by Oasis IT Services.

17.4 It is recognised that staff members may wish to share their experience, expertise and personal interests with a wider audience through the use of personal blogs. Staff are advised to consider carefully the implications of the publication of personal information on the internet and ramifications of this being available within their professional lives. The publication of information relating to OCL in any way including details of employment may only be shared with the explicit permission of the line manager. Any publication of materials in a personal capacity must be explicitly identified as such.

18. Newsgroups, Forums and Personal Websites

18.1 The internet provides access to a very large number of Newsgroups and Forums which allow individuals to communicate and discuss particular topics. Many of these areas are unmoderated and the content can differ significantly from the reported purpose of the site. Access to these

sites is blocked by default. Access to these sites from within the Oasis network will only be granted as per the Oasis Web Filtering Changes Policy.

18.2 Newsgroups and Forums can form a useful source of information and research and research of particular topics and also provide an environment for the formation of positive contact with subject matter experts. However, they are also prone to abuse and misinformation and can also provide an environment for harassment and manipulation of vulnerable individuals. As part of the Oasis Online Safety Curriculum students will be instructed about access to these sorts of sites including being given an understanding of the risks and guidance on their safe use.

18.3 The development of websites is a useful skill and Oasis recognises the benefits to students in developing web development skills. However, the publication of personal information as part of the design and development of a personal website can place the student at risk from exploitation.

18.4 The development of public websites as part of the curriculum should be included in medium term planning and discussed with academy principals before it is undertaken with students.

18.5 Oasis IT Services can provide facilities for students to self-publish websites which are available exclusively within the Oasis IT Network and externally if required. It is recommended that this is considered as a publication mechanism in planning.

18.6 The class teacher must put in place effective processes to ensure that they are moderating any content that is published, being mindful at all times of the E-safety implications of the publication of personal information and are in a position to edit or remove content that has been published as part of the site without reference to the student.

18.7 It is recognised that staff members may wish to share their experience, expertise and personal interests with a wider audience through the use of Newgroups, Forums and Personal Websites. Staff are advised to consider carefully the implications of the publication of personal information on the internet and ramifications of this being available within their professional lives. The publication of information relating to OCL in any way including details of employment may only be shared with the explicit permission of the line manager. Any publication of materials in a personal capacity must be explicitly identified as such.

RACI matrix

Policy Element		Leadership			Academy							National Services & IT Directorate Teams														
	Policy Owner	OCL CEO	OCL COO	Regional Director	Academy Principal	Designated Representative	Designated Data Protection Lead	DSL	Teacher	Academy Staff User	Student	Head of National Services	National Service User	Director of Information Technology	Head of Service Delivery	National Infrastructure Manager	National Programme Manager	National IT Operations Manager	National Safeguarding Lead	Data Protection Officer	Business Relationship Manager	National Service Desk Manager	National Service Desk	Service Delivery Manager	Cluster Manager	Onsite Teams
6.3 Adherence to IT Security Policy (Academy)	R	R	R	R	R		C			A		R		C	C	C	C		C	C	C	C	C	C	C	C
6.3 Adherence to IT Security Policy (National)	R	R	R									R	A	C	C	C	C		C	C	C	C	C	C	C	C
6.4 Educating Students in Online Safety		R		R	A	R		C	R					C					C					C		
6.4-5 Supporting Parents in E-Safety		R		R	A	R		C	R					C					C	C				C		
7.1-2 Understanding the Policy (Academy)				R	R			C		A				C						C				C		
7.1-2 Understanding the Policy (National Office)			R									R	A	C						C				C		
7.3 Technical Controls			R	C	C	C		C	I	I	I	C		A	R	R			C	C	C	I	I	C	I	I
7.4 Training for Staff, Students and Parents		R		R	A	R		C	R	R				C	C				C	C				C		
7.5 Enrolment in the Safer Schools App		R		R	A			R	I	I	I								C							
7.6 – 7 Acceptable Use Agreements		R	R	R	A	R		C	I	I	I															
7.8 Process for dealing with E-Safety Breaches		R		R	A	R		R	I	I	I			C	C				C			I		C	I	I
8.4 Information for Parents about E-Safety and Horizons		R	R	R	A	R		R	I	I	I			C	C				C	C				C		

8.5 Jamf Parents App		I	I	I	C	R		I	I	I				A	R	R			C	C	C	R	R	R	I	I
9.4, .7, .11 Monitoring of Filtering Reports / Online Activity		R		R	R	R		A	C	C				R	R	R			C	C		C	C	C	C	C
9.12 Implementation of Safe Search		I	R	I	I	I		I	I	I		I		A	R	R			C	I		I	I	I	I	I
10.1-.3 Acceptable Use (Academy)		R		R	R		C	C		A																
10.1-.3 Acceptable Use (National)			R									R	A													
10.4 Management of Unacceptable Use (Student)		R		R	A	R	C	I	I	I	I													C		
10.4 Management of Unacceptable Use (Staff, Academy)		R		R	A	R	C	I	I	I	I			C	C							C	C	C		
10.4 Management of Unacceptable Use (Staff, National)			R									A		C	C							C	C	C		
10.5 Student Mobile Phone Use		R		R	A	R	C	I	I	I	I															
11.2 Sharing of Account Information (Academy)										A																
11.2 Sharing of Account Information (National)													A													
11.4 Shared Class Accounts		R		R	A	R		C		R				C	C							I	I	I	I	I
11.2 Account Information (Academy)										A																
11.2 Account Information (National)													A													
14.6 Training for staff in using MS Teams		R		R	A	R	C	I	I	I	I			C	C									C	C	I
14.9 Recording Student Interaction in MS Teams		R		R	A	R	C		R	R	I													C	C	C
16.2 Access to Video Services					A	C	C		I	I	I			C	C	R						R	R	C	C	I
18.3 – 6 Student Use of Personal Website Publishing Services		R		R	R	R	C		A	I	I				C	C						C	C	C	C	I

Document Control

Changes History

Version	Date	Owned and Amended by	Recipients	Purpose
9.3a	20/09/2020	Liz Hankin	Rob Lamont, Marc Hundley	Verify edits
9.3b	30/09/2020	Liz Hankin	Rob Lamont, Marc Hundley	Verify edits
9.3c	06/10/2020	Liz Hankin	Rob Lamont, Marc Hundley	Verify edits, complete RACI matrix
9.3	11/11/ 2020	Liz Hankin	Rob Lamont	Final edits re email and updated RACI matrix with Online Safety Lead
9.4	05/03/2021	Liz Hankin	Rob Lamont	Updated to match Oasis Horizons etc
9.5	16/03/2021	Liz Hankin	Rob Lamont	Updated to match remote learning
9.6	04/05/2021	Jill Rowe	Rob Lamont	Updated Introduction

Policy Tier

☒ Tier 1

☐ Tier 2

☐ Tier 3

☐ Tier 4

Owner

Rob Lamont

Contact in case of query

rob.lamont@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
Directors Meeting		10.05.21	9.6

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
Rob Lamont	Director of Information Technology	16/03/2021	9.5