E-SAFETY POLICY

E-Safety Policy
V11.0
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.

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.

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.

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 and personal development 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.

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.

Checklist

- ❑ We will agree to comply with the restrictions, filtering and monitoring put in place to keep all users of Oasis IT systems safe.
- ❑ We will ensure that Academy Leadership Teams can provide academy-led education and information to ensure all users are appropriately informed of the contents of this E-Safety Policy through age-appropriate resources.
- ❑ We all need to make use of a range of technologies at work and in our personal lives. To keep as safe as possible Oasis will provide all users including students, with annual E-Safety Training.

- ❑ We have produced the IT Security and Acceptable Use of Technologies Policies to support this E-Safety Policy. Security and E-Safety concerns are closely linked, so it is essential all users have these Policies explained, issued and agreed by the different users of the Oasis system and equipment as part of their personal development programme.
- ❑ We have provided Academies with access 'Safer Schools App'. All academies must enrol for use of the app and that its use has been actively promoted to parents and students (from Key Stage 2 – Key Stage 5).
- ❑ We will be monitoring the DfE 'Keeping Children Safe in Education' guidance document for schools and colleges and will ensure that academies receive advice on any changes to requirements.
- ❑ We will take every opportunity to help students and their parents/carers understand E-Safety issues through 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.

In brief

This E-Safety Policy applies without exception to all users of Oasis IT systems, 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.

Academy application of and compliance to E-Safety Policy

- Appendix 1 (Sections 1a – 1i) contains technical and organisational requirements for implementing and compliance with this policy.
- Appendix 2 (Sections 2a – 2i) contains an overview of the level of knowledge and understanding of E-Safety relevant to all users for acceptable and safe use of Oasis IT system and personal technologies and the content should form part of personal development training.
- 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.
- 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.
- To assist academies in supporting parents/carers, Oasis has provided a series of resources based on how they can approach online safety with the child/children. Each academy has access to these resources through the Safeguarding page on their academy website. There is a section devoted to parents/carers.
- To support compliance with this policy, an academy must ensure that all students are actively supported in the development of the skills and knowledge

to remain safe whilst using technology and when online. The Oasis Online Safety Curriculum Policy is provided to support this process and includes resources to educate young people in the safe use of technology.

- Appendix 3 provides an overview of the Oasis Online Curriculum Policy and links to Oasis Safeguarding E-Safety resources are provided in Appendix 3 to assist academies with their planned implementation.

Specific E-Safety guidance for use of technologies

The following uses of technologies have been identified as those that could raise E-Safety concerns or require specific attention.

Responsibilities

- Individual users are responsible for making sure that they understand what their role and responsibilities for use of IT entails. For children aged 12 or younger this responsibility falls to the parents/carers.
- 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.

- 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.
- The 'Acceptable User Agreement' forms the agreement between any authorised user of Oasis IT systems and Oasis. Oasis has a standard Acceptable Use of Technologies Policy which applies to all users of the system.
- 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.
- Academies must put in place processes to detail how any breaches of the E-Safety Policy will be documented, reported and dealt with.

Training requirements

- Academy Leadership Teams will develop a process for all users to receive annual academy-led E-Safety and Online Safety Training. OCL has developed resources that can be used for academy-led training sessions.
- To comply with 'Keeping Children Safe in Education' (KCSIE) document for schools and colleges, all authorised staff users need to be familiar with the relevant content within this document.
- Provision should be made by Academy Leadership Teams to support Parents/Carers with access to and use of the 'Safer Schools 'App.
- Oasis IT Cluster Managers must ensure that the IT Cluster technicians are confident with the application and processing of the monitoring and filtering system in place.

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 2021

Oasis staff with 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 Use of Personal Devices Policy 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 E-Safety Policy.
- The contents of this document are fully compliant with the DfE statutory guidelines KCSIE. The legal requirements of the KCSIE guidelines are consistent with those designated as mandatory within this document.
- 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.
- Appendices 1b and 3 contains links to websites and resources that can assist Academy Leadership Teams in selecting age-appropriate resources to support the development of the Oasis Online Safety Curriculum implementation and compliance with KCSIE.
- Appendix 2a contains links that can be shared with Parent/Carer and students to help them understand personal E-Safety procedures and actions.

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 will agree to comply with all restrictions, filtering and monitoring put in place to keep all users safe	I	I	I	I	I	I	C	C	C	C	R	R	R	A	C	C	I	C	I
We will ensure that Academy Leadership Teams can provide education and information to ensure all users are informed of the content of this E-Safety Policy	I	I	I	C	C	C	C	I	I	A				C	I	I	I	I	I

All users will be provided with annual E-Safety and Online Safety Training relevant to their age and role	I	I	C	I	I	C	A	I	I	R	R	I	I	C	I	I	I	C	I
All users and parents/carers will be informed of the content of IT Security and Acceptable Use of Technologies Policies to make sure that they are compliant with this E-Safety Policy	I	I	I	I	I	C	C	I	I	A	R	R	R	C	C	C	I	C	I
All academies will be enrolled for the use of the 'Safer School App' that is actively promoted for parental/carer use by the academy	I	I	I	I	I	I	A	I	C	A	R	I	I	A	C	C	C	I	I
We will monitor the DfE KCSIE guidance and inform academies of any changes in requirements.	I	I	I	I	I	C	R	C	C	I	I	I	I	R	I	I	I	I	I

APPENDIX 1 Technical and Organisational E-Safety requirements

1a Related Oasis Policies

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 Parental & Carer Code of Conduct Policy
- The Oasis Trips and Visits Policy
- The Oasis Device Monitoring Policy
- The Oasis Web Filtering Policy
- The Oasis Data Protection Policy
- Use of Email 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
- Oasis CCTV Policy

1b Additional academy support resources for online safety

Keeping Children Safe in Education resource links

Childnet provide guidance for schools on cyberbullying.
Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation.
NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements.
Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective.
Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones.
South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements.
Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.
Online safety guidance if you own or manage an online platform
DCMS advice A business guide for protecting children on your online platform DCMS advice
UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online.

Support for remote education, virtual lessons and live streaming

Guidance: Get help with remote education resources and support for teachers and school leaders on educating pupils and students.
Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely.
London Grid for Learning guidance, including platform specific advice.
National cyber security centre guidance on choosing, configuring and deploying video conferencing.

Oasis online academy resources
Age-appropriate E-Safety resources - Oasis E-Safety resources.
Age-appropriate Cybersecurity resources - Cybersecurity resources.

1c E-Safety and Oasis Horizons

- 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.
- 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.
- 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, including the deployment of the 'Safer Schools App'.
- Oasis IT Services have made the 'Jamf' Parents App 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.

1d Managing Internet Access, Monitoring and Filtering

- 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.
- 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.
- 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.
- 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.

- Oasis implements 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.
- 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.
- 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.
- 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.
- 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.
- Offsite filtering is applied uniformly to all academies. Different filtering can be applied to primary and secondary students and for staff.
- Oasis IT Services provide a dashboard for Academy DSLs which highlights blocked activity carried out on a device when it is used.
- 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.
- 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.
- 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.

1e Student Accounts and Passwords

- 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.
- Passwords will be applied as per the Oasis Password Policy.
- The use of shared accounts or class accounts is not permitted for students who are in year one or higher.
- 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.

1f Managing Personal Data, Video Conferencing, Chat & Instant Messaging

- The management of all personal data relating to staff and students must be conducted in accordance with the Oasis Data Protection Policy.
- 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.
- 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.
- 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.
- 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.
- The use of 'cameras' as part of the delivery of online and remote learning is encouraged 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.
- 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.

1g Managing use of Social Media and Video Sharing sites

- 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.
- The tools provided within the Oasis IT system and OCL Online Safety Curriculum 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.
- 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.
- 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.
- Academies are encouraged to operate official social media channels to communicate with the wider academy community.
- 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.
- It is recognised that staff may wish to make use of social media in their personal lives.
- 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.
- 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.

1h Managing use of Blogs

- 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.
- 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 deemed to be inappropriate then the IT Service Desk should be notified immediately so that access can be restricted.

1i Managing use of Newsgroups, Forums and Personal Websites

- The development of websites is a useful skill and Oasis recognises the benefits to students in developing web development skills whether related to a curriculum requirement or personal interest. 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.
- 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.
- 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.
- 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 are instructed about access to these sorts of sites including being given an understanding of the risks and guidance on their safe use.
- 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.

APPENDIX 2 E-Safety for all users of Oasis IT systems

2a Online safety parental and student support resources

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support.
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents.
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying.
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world.
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation.
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online.
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online.
- Parentzone provides help for parents and carers on how to keep their children safe online.
- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment.
- #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships.

2b Unacceptable use of computers, mobile devices (including phones) and network resources

- 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.
- 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.
- 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).

- 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.
- 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.
- 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.
- 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.

2c Student Accounts and Passwords

- 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.
- 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.
- 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.

2d Email

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

- 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.
- Students who choose to misuse the email system will be subject to disciplinary procedures as outlined in the Behaviour for Learning Policy.
- Staff who choose to misuse the email system may be subject to disciplinary procedures.
- 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.
- Personal email or messaging between staff and students is forbidden.
- Students in KS1 (Reception, Year 1 and Year 2) have mail flow restrictions in place restricting email to internal only. KS1 Students cannot send emails to external recipients and cannot receive emails from external senders. Students in Year 3 and above have no mail flow restrictions and can therefore send and receive email internally and externally.

2e Personal Data, Video Conferencing, Chat & Instant Messaging

- 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.
- Video Conferences/online meetings must include a member of staff who is responsible for moderating the behaviour and conduct of all participants.
- 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.
- 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.
- Oasis IT Services can retrieve chat/instant message conversations undertaken using the Microsoft Office 365 environment.
- 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.
- 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.

2f Use of Social Media

- Staff are advised to carefully consider 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.

- 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.
- It is recognised that staff may wish to make use of Social Media in their personal lives. Staff are advised to carefully consider 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.

2g Use of Video Sharing Sites

- 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.

2h Use of Blogs

- 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.
- 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.

2i Use of Newsgroups, Forums and Personal Websites

- 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 able to edit or remove content that has been published as part of the site without reference to the student.
- It is recognised that staff members may wish to share their experience, expertise and personal interests with a wider audience using 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.

APPENDIX 3 Overview of Oasis Online Safety Curriculum Policy

The full version of the Oasis Online Safety Curriculum Policy and linked resources is available from the Oasis Policy Portal.

To support planning and implementation of the Online Safety Curriculum , age-appropriate resources are available through the OCL – Safeguarding SharePoint site: https://oasisit.sharepoint.com/sites/OCL-EDU-SG/SitePages/eSafety.aspx

Key aspects for management of the Online Safety Curriculum

- Online safety curriculum leadership.
- Leadership of online safety curriculum should not be given to the teacher leading Computing. This role must go to a senior leader with an overview of the academy's curriculum. This leader must ensure that they work hand in hand with the DSL to ensure that all statutory requirements are fully in place.
- Curriculum planning.
- Teaching on online safety should generally be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching must always be age and developmentally appropriate.
- Documented curriculum mapping.
- Each academy must have a clear, documented curriculum mapping for delivering online safety curriculum in each year group based on the content of the Oasis Online Safety Guidance Notes. The curriculum mapping should indicate the content that will be covered, when during the academic year the sessions will take place, if they are within specific subjects or specific events planned to support the knowledge and experience.
- The curriculum mapping will be agreed with the academy Regional Director.

Academy wide approach

- Whole-school approaches are likely to make teaching more effective than lessons alone. A whole academy approach is one that goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.
- The Designated Safeguarding Lead holds responsibility to ensure the curriculum meets the contextual on-line safety needs of the academy.
- To truly embed teaching about online safety and harms within a whole school approach, in practice, this means an academy must:
- Create a culture that incorporates the principles of online safety across all elements of academy life. The principles should be reflected in the academy's policies and practice where appropriate, and should be communicated with staff, students and parents / carers. It will also include reflecting online behaviours in the academy's behaviour and bullying policies. Students should be just as clear about what is expected of them online as offline.
- Proactively engage staff, students, parents or carers in academy activities that promote the agreed principles of online safety. Involving the co-design of programmes to ensure the academy captures information from parents / carers and students about their experience of emerging issues they are hearing about or facing online creates an atmosphere of trust.

- Ensure staff have access to up-to-date appropriate training/CPD and resources, so that they are confident in covering the required content in a way that is relevant to their students' lives. Establishing an item on staff meeting agendas to cover developments in online safety, led by the Online Safety Lead, creates a structured approach to distributing updates.
- The chosen administrator for the 'Safer Schools App' will ensure that the on-line safety messages created within the app are distributed appropriately.
- Reinforce what is taught in lessons or events by taking appropriate and consistent action when a student makes a report of unacceptable online behaviours from another student, including cyberbullying, or shares a concern about something they have seen online.
- Model the online safety principles consistently. This includes expecting the same standards of behaviour whenever a student is online at the academy - be it in class, logged on at the library or using their own device in the playground.
- Extend support to parents / carers, so they can incorporate the same principles of online safety at home.

Online Safety Curriculum content

- The Oasis Online Safety Curriculum Guidance Notes provide a breakdown by category, and by age-appropriate criteria.
- Full details of the scope for each of the defined content areas can be found in the Oasis Online Safety Curriculum Guidance Notes.
- The Oasis Online Safety Curriculum Guidance Notes will be frequently updated as new content becomes available. The Academy Lead for Online Safety will be informed of updates and changes as they are made to the document(s) and must update the academy curriculum mapping in line with changes.
- Due to the frequency of change required to maintain up to date content for the online safety curriculum access to resources such as the Safer Schools App, with its on-line safety support, and the CEOPS reporting tool has been made available to pupils, parents/carers and staff through Oasis Horizons. The content areas that are to be mapped by an academy are:
    - Underpinning knowledge and behaviours.
    - How to navigate the internet and manage information.
    - Managing information online.
    - Copyright and ownership.
    - Privacy and security.
    - Online relationships.
    - Self-image and identity.
    - Online reputation.
    - Health, well-being and lifestyle.
    - Personal safety.

Oasis online academy resources

- Age-appropriate E-Safety resources - Oasis E-Safety resources.
- Age-appropriate Cybersecurity resources - Cybersecurity resources.

Document Control

Changes History

Version	Date	Owned and amended by	Recipients	Purpose
10.0	09/12/2022	Mark Thornton, Liz Hankin, Jon Needham	Mark Thornton	Updated and reformatted
11.0	26/04/2023	Mark Thornton, Liz Hankin, Jon Needham	Mark Thornton, IT Directorate Senior Managers	Updated and edited in line with OCL policy template

Policy Tier

☒ Tier 1
☐ Tier 2
☐ Tier 3
☐ Tier 4

Owner

Mark Thornton

Contact in case of query

Mark Thornton, Director of IT, mark.thornton@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
Approval at directors' group is not required, as this is a review	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
Mark Thornton	Director IT	12/12/2022	V10.0
Mark Thornton, IT Directorate Senior Managers,	Director IT, Senior Management Team	26/04/2023	V11.0