



E-SAFETY POLICY

April 2021

Updated internally by E-safety Lead – September 2022

CONTENTS

1.	Introduction and the Oasis Vision, Ethos and 9 Habits	3
	<i>The Oasis 9 Habits</i>	3
	<i>Introduction</i>	4
2.	What is this policy about?	4
	<i>In brief</i>	4
	<i>In more detail</i>	5
3.	Who is this policy for?	5
4.	The requirements that apply to this policy	5
	<i>Applicable legislation</i>	6
5.	Policy Scope	6
6.	Academy application of and compliance to E-Safety Policy	7
7.	Roles and Responsibilities	7
8.	E-Safety and the Oasis Horizons Project	8
9.	Internet Access, Monitoring and Filtering	8
10.	Unacceptable use of computers, mobile devices (including phones) and network resources	10
11.	Student Accounts and Passwords	10
12.	Email	11
13.	Publication of Personal Data	12
14.	Video Conferencing, Chat & Instant Messaging	12
15.	Social Media	13
16.	Video Sharing Sites	14
17.	Blogs	14
18.	Newsgroups, Forums and Personal Websites	14
	RACI matrix	16
	Appendix 2 - Operational E-Safety Manual Template	24
	Appendix 3 - Reference - Whole Academy Operational E-Safety matrix and sanctions	34
	Appendix 4 – Reference - Roles and Responsibilities	42

Appendix 5 – Reference - Acceptable Use of Technology Agreements	45
Appendix 6 – Reference - Flow Diagram E-Safety incident reporting.....	51
Appendix 7 – Guidance - Age appropriate agreement discussion & Rules for Students	52
Appendix 8 – Guidance - Use of technologies around Oasis Academies	55
Appendix 9 – Guidance - Sample Home Use Agreement - Oasis equipment.....	58
Appendix 10 – Guidance - Developing safe use of Learning Technologies	59
Appendix 11 – Guidance - Oasis IT Frameworks for developing use of Learning Technologies	60
Appendix 12 – Guidance - E-Safety within other Oasis Policies.....	63
Appendix 13 - Guidance - Biometrics Information for Parents	69
Document Control	18

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 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 policies is considered to be an offence and in that event, Oasis Trust disciplinary procedures will apply

- [Copyright, Designs and Patents Act 1988 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Malicious Communications Act 1988 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Computer Misuse Act 1990 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Criminal Justice and Public Order Act 1994 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Trade Marks Act 1994 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Data protection – GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Human Rights Act 1998 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Regulation of Investigatory Powers Act 2000 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Freedom of Information Act 2000 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Communications Act 2003 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Criminal Justice and Immigration Act 2008 \(legislation.gov.uk\)](http://legislation.gov.uk)
- [Keeping children safe in education \(2020\) – GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Guide to General Data protection Regulation – GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Prevent review \(publishing.service.gov.uk\)](http://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 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 3G/4G/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 Newsgroups, 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

Appendix 2 - Operational E-Safety Manual Template

To support academies in creating their own operational E-Safety Manual the following Template covers the required contents. Each academy should produce their own version of the document with relevant decisions about the implementation of the procedures within the academy. The table indicates where supportive guidance can be found to assist the production of the academy document. All sections are mandatory and where possible the document has been populated with content that does not require academy decisions.

A standalone copy of the template is available as a separate document for completion.

Aspect of Manual	Information
1 Top Level Overview <ul style="list-style-type: none"> Academy strategy for use of Technologies 	Academy statement of vision for use of technologies and embedded E-Safety programme Guidance: E-Safety Policy Appendix 10 Developing safe use of learning technologies
<ul style="list-style-type: none"> Procedures for use of Technologies around the Academy 	Guidance: E-Safety Policy Appendix 8 Use of technologies around Oasis Academies

<ul style="list-style-type: none"> Acceptable use of Technologies Agreements: <ul style="list-style-type: none"> Oasis Staff Oasis Students 	<p>Reference: E-Safety Policy Appendix 5 Acceptable User Agreements Guidance: E-Safety Policy Appendix 7 Resource for discussing Agreement with Reception, Key Stage 1 students</p>
<ul style="list-style-type: none"> Home Use Agreement – Oasis equipment 	<p>Guidance: E-Safety Policy Appendix 9 Sample Home Use Agreement – Oasis Equipment</p>
<ul style="list-style-type: none"> Biometrics Parent/Carer information and Opt-in Form 	<p>References: E-Safety Policy Appendix 13 Biometrics Parent/Carer information Parent/Carer Opt-in Form</p>
<ul style="list-style-type: none"> Use of Personally Owned Devices 	<p>References: E-Safety Policy Use Personally owned devices</p>
<p>2 Whole Academy planning for E-Safety</p>	<p>Reference: E-Safety Policy Appendix 3 Checklist for whole Academy E-Safety procedures Guidance: E-Safety Policy Appendix 11</p>

	Oasis IT Services Learning Technology Frameworks
3 Academy procedures for Incidents, escalation points and sanctions	References: <i>E-Safety Policy</i> Appendix 3 Decisions for acceptable and unacceptable use, sanctions and communications technologies Appendix 6 Flow Diagram E-Safety incident reporting
4 Roles and responsibilities	Reference Page: <i>E-Safety Policy</i> Appendix 4 Checklist Roles and Responsibilities
5 Risk analysis / Risk Register	Reference: Risk Analysis Risk Register

Academy strategy for the use of Technology

Top Level Academy statement of vision for use of technologies and embedded E-Safety programme and should include reference statements to explain how academy will support and apply: Procedures for use of Technologies around the Academy Acceptable use of Technologies Agreements:

- Oasis Staff
- Oasis Students
- Use of Oasis equipment at home (if appropriate)
- Biometrics Parent/Carer information and Opt-in Form
- Use of Personally Owned Devices (in accordance with OCL UPOD Policy)

At Clarksfield, we use a whole school approach to **e-safety** which helps ensure staff and parents are able to **teach** children about staying **safe** when using internet technologies. It also helps make sure pupils themselves know how to behave responsibly **online**.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy's e-safety Policy (using technology within the Academy, as well as at home)
- When accessing, amending and saving any data or information, relating to the Academy or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.
- All internet activity within school is monitored and filtered through the Smoothwall system. Whenever any inappropriate use is detected, the e-safety lead is notified and the incident will be followed up in line with the Academy's Acceptable Use Policy.
- The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school's digital devices.
- If Internet research is set for homework, staff will remind pupils of their e-safety training. Parents are encouraged to support and supervise any further research.
- Staff are not permitted to bring in personal mobile phones and devices **to use in the classroom**

Our E-Safety programme will ensure that:

- staff and volunteers are confident in online safety, identifying and responding to concerns
- children and young people are taught the skills to stay safe online
- helpful advice and resources are shared with parents and carers through online resources on the school website and off-line resources linked to learning.
- robust e-safety policies and procedures are developed, and that effective IT infrastructure and support is in place
- as an Academy, we regularly review and improve our e-safety provision

2 Academy wide E-Safety procedures

2.1 OVERVIEW

Top level statements about how academy will ensure an understanding and application of responsibilities relating to use of technologies in and around the academy

At Clarksfield, we build in the use of technologies in order to equip our young people with the skills to access life-long learning and employment. E-safety involves pupils, staff, governors and parents making best use of technology, information and training to create and maintain a safe online and ICT environment at our Academy.

The E-Safety Lead:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy's e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Pupils:

- Rules for Internet access are posted in all classrooms.
- Pupils are informed that Internet use will be monitored.
- Pupils are informed of the importance of being safe on social networking site. This is strongly reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons.
- Pupils sign an age appropriate Acceptable Users Policy, which is accessible to parents through the school website.
- Pupils are informed on how to report incident in situations both inside and outside of school.

Staff:

- All staff are given the Academy e-safety Policy and its importance is explained
- All staff sign an Acceptable users policy

Parents:

- Parents' attention is drawn to the Academy e-safety Policy in newsletters and on the Academy Website
- Parents have access to a copy of the pupils acceptable users policy via the school website.
- Parents are made aware of their responsibilities in regards to school technologies that are available for use in the home (Student iPads – The Horizons Project)
- Parents have links to training to support childrens use of technology, made available through the school website.

2.2 SUPPORT FOR STAFF E-SAFETY PROCEDURES

Statements should include how staff will be trained, supported in their understanding will be issued, displayed and applied

Whole school safeguarding training includes elements of eSafety.

At every staff meeting, staff are given a 5 minute brief around safeguarding (key messages and updates) this also includes eSafety.

Annually, staff complete the HAYS and Prevent online modules and the modules include eSafety training as well as important updates.

Staff agree to the OCL Acceptable User Policy every time they log on to their laptops.

2.3 SUPPORT FOR STUDENTS E-SAFETY PROCEDURES

Statements should include how students will be taught E-Safety issues contained within the Oasis E-Safety Policy, how the rules applying to E-Safety will be upheld and how student rules issued, displayed and applied

At Clarksfield, E- Safety is taught through the curriculum (as part of the Computing curriculum). The E - Safety content ensures that our pupils use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact. All pupils have signed a child friendly acceptable user policy (which has also been shared with parents), and they

2.4 ACADEMY STATEMENTS RE STUDENTS USE OF:

2.4.1 *Internet*

Smooth wall and Future digital are used to monitor online activity (for both children and staff). Children are made aware of the Academy's expectations when using the internet to access websites. Any pupils not following the Academy's expectations, consequences as per the E- Safety policy. Access to inappropriate websites is blocked.

2.4.2 *Email*

Pupils have access to Outlook and Teams, use is monitored

2.4.3 *Webmail*

Pupils do not have access to webmail in school

2.4.4 *Chat Rooms*

Pupils do have access to chat rooms in school but only on pre-approved apps and when directed by an adult.

2.4.5 *Instant Messaging*

Pupils do have access to instant messaging in school but only on pre-approved apps and when directed by an adult.

2.4.6 *Mobile phones/portable devices*

Pupils have access to iPads and other portable technologies in school, use is monitored.

2.4.7 *Camera phones*

Pupils do not have access to camera phones in school

2.4.8 *Webcams*

Pupils do have access to webcams in school but only on pre-approved apps and when directed by an adult.

2.4.9 *Peer to peer networks*

Pupils do not have access to peer to peer networks in school

2.4.10 *Third-party supplied sites*

Smooth wall and Future digital are used to monitor online activity (for both children and staff). Children are made aware of the Academy's expectations when using the internet to access websites. Any pupils not following the Academy's expectations, consequences as per the eSafety policy. Access to inappropriate websites is blocked.

Appendix 3 - Reference - Whole Academy Operational E-Safety matrix and sanctions

Operational procedures

When formulating Academy-wide operational procedures:

Does the Academy have a suite of up to date E- Safety operational procedures that comply with the Oasis E-Safety, Acceptable use of Technologies and Use of personally Owned Devices Policies? Yes
Are a wide range of users consulted when policies are being reviewed, re-written? Yes – Inset
Who is responsible within Oasis Academy for E-Safety operational procedures? - Alex Unwin
Are all users familiar with the Oasis E-Safety Policy and the Academy Operational E-Safety Document? Yes
Are there clear rules and guides visible in areas where students access technologies? – Yes
Do all users know how to report incidents, such as inadvertent access to undesirable websites/images? Yes – Bromcom and CPOMS if it is a serious safeguarding concern
Are there clear links from the E-Safety procedures to those within other Policies, such as Safeguarding, Behaviour for Learning Policy, Curriculum Policies, Teaching and learning Policies, Anti-Bullying Policy? Yes
Do all users know what sanctions could be applied for misuse of Oasis IT systems and equipment? Yes – Sanctions Matrix
Are Oasis E-Safety procedures and reports regularly reviewed within school? Yes

Operational E-Safety staff support

Decisions about how staff will be trained, supported in their understanding will be issued, displayed and applied

Do staff receive information and training on E-Safety and new emerging technologies on a regular basis? - Yes – E-safety newsletters, Training Updates, Computing Curriculum, E-safety leadership
Is training directed to their specific role in the Academy? - Yes
Is there a clear process for supporting staff in the E-Safety development? - Staff should contact the computing and e-safety lead for support and guidance in procedures, policies and the teaching of e-safety
Is there a clear process for staff to report any difficulties or concerns they may encounter? – Yes, report to E-safety Lead, DSL
Do staff receive training on information literacy skills? For example, how to search and evaluate validity of information effectively? - Yes through teaching of Computing Curriculum which covers those topic areas.
Do new staff have an introduction to the Oasis E-Safety Policy and the Academy Operational ESafety Document as part of their induction? – Yes
Are staff expected to incorporate E-Safety activities and awareness within their curriculum areas? – Yes – Computing Curriculum
Are the E-Safety activities and awareness sessions monitored, co-ordinated and supported across the Academy? Yes

Operational E-Safety student support

Decisions about how students will be taught E-Safety issues contained within the Oasis E-Safety Policy, how the rules applying to E-Safety will be upheld and how student rules issued, displayed and applied

E-Safety Policy
(V9.2/ July 2018)

(IT Business Relationship Manager/ Review: November 2019)

Are students given an opportunity to contribute to Academy E-Safety procedures? No
Are students and their parents/carers provided with access to a copy of the Oasis E-Safety Policy and the Academy Operational E-Safety Document when the student joins Oasis? – Yes – policies section of school website
Do you know about a student's prior exposure to technologies? Yes, through information gathering as part of the curriculum
Do students see the E-Safety rules for use of Academy IT equipment, the Oasis Microsoft Office 365 and tools, and the internet each time they use technology? Yes – All staff to add Acceptable use policy to the beginning of all teaching presentations.
Does the Academy have a framework for teaching E-Safety skills? Yes – Oasis One Curriculum
Does the Academy provide appropriate opportunities within a range of curriculum areas to teach E-Safety? Yes. – Cross-Curricular Curriculum Links.
How does the Academy go about educating students of their exposures to the dangers of technology outside of Academy? – E-safety section on website with addition information.
How is students' understanding of E-Safety issues assessed or measured? Continually accessed through teaching of computing.
Are students aware of relevant legislation when using the Oasis Microsoft Office 365 and tools, and the internet, such as that relating to data protection, intellectual property, which may limit what they might want to do, but also serves to protect them? Yes, taught within the curriculum.
Are students aware of the impact of online bullying, from the perspective of both the victim and the tormentor? Yes – Covered within the Computing Curriculum and Addressed as part of PSHE.
Do they know how and where to seek help if they are affected by online bullying? Yes – Covered within the Computing Curriculum and Addressed as part of PSHE

Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Internet
What are the restrictions placed on internet use within Academy? For example, do students know the rules about access the internet on personal devices within school? Yes – Firewalls, Smoothwall, search filters. No students are allow personal devices. Sanctions matrix.
Are there individual logins to all accessible websites and security time-outs? Yes, secured by Secure keys with two factor authentication and timed log outs.
Does the Academy use a safe list of websites? Yes – Centrally Blocked through smoothwall. Children also have access to pre-vetted apps that are only available through a closed system, app stores are unavailable both in and out of school.
Are students taught how to critically evaluate materials as well as learning good searching skills? Yes – computing curriculum
Are students taught the importance of intellectual property regarding materials they find on the internet? Yes – Computing Curriculum
Are students aware of the Academy's policy on downloading materials from the internet? Downloading is restricted on devices.

Are there different guidelines for different types of materials – for example, copyright-free materials to support classroom work can be downloaded, but downloading of games and music is prohibited? – Children can download preapproved games and applications through the closed self-service, but apps are restricted when on school network.
Email
Do students have access to email in the Academy? Is this applied by the account permissions or Academy requested access? Yes – outlook email.
If students do have an individual email address in the Academy, do they understand any restrictions on use? For example, can it be used for work-related correspondence only or for personal use? Yes – children should be introduced to and informed of expected and acceptable use when first signing into email. – Children are taught to use emails as part of the curriculum.
How is student email use monitored, and are students aware of this? Centrally managed, children are aware that activity is monitored through remote software and live activity can be seen through apple classroom.
Are students aware of the Academy's policies on email attachments? Will be taught through the curriculum. Children should only be attaching documents, etc under the direction of the person leading the class or activity.
Do students know how to virus-check attachments, both incoming and outgoing? Yes, through computing curriculum teaching about validity, scams and phishing.
Are students aware of the seriousness of bullying by email? Yes
Is this incorporated in the Academy's anti-bullying policy? Yes
Are all students aware that there are sanctions for misuse of email on the Oasis network? Yes – children are made aware through acceptable users policy.
Webmail
Do students know Oasis' policy on webmail services? Webmail is not to be used by students, access through app only.
Do students know how to use webmail services safely outside the Academy, for example by looking for privacy statements when registering for webmail accounts? Yes, children are taught this as part of using Email services.
Do students know how to use inbuilt junk mail filters within webmail services? Yes – children are shown how to filter, search and mark emails.
Are students aware of the issues surrounding spam and spoofing? Yes, children are aware.
Are students taught appropriate strategies for recognising and dealing with spam? Yeas, through e-safety in the curriculum.
Are instructions given within the Academy to help minimise spam? Yes – through the curriculum.
Chat Rooms
Are students aware of the safety issues relating to using chat rooms? Yes- PSHE and e-safety in the computing curriculum
Are students aware how to safely negotiate online relationships? Yes- PSHE and e-safety in the computing curriculum
Are students aware of the importance of keeping personal information private when chatting? Yes- PSHE and e-safety in the computing curriculum

Are students aware of the dangers of arranging offline meetings with people they have met online? YES – PSHE
Is use of any chat room permitted within the Academy? If so, is this for classroom use only? Yes, children can use some services on preapproved websites, apps and teams, however use is limited too teachers discretion.
Instant Messaging
Is access to instant messaging services permitted within the Academy? For example, the classroom uses of Skype for Business. Yes
Are students aware of the safety issues relating to instant messaging? Yes – PSHE and E-safety in the computing curriculum.
Do students know how to protect personal information when registering for instant messaging services, and how to set up closed groups or buddy lists? Yes – through computing curriculum.
Do students know where to get help and advice if they experience problems such as unwanted messages or bullying by instant messaging? Yes – PSHE and E-safety in the computing curriculum.
Mobile phones/portable devices

Does Academy policy allow students to have personally owned mobile phones/mobile devices with them in school? (Such a policy requires approval from a Regional Director) No
If Academy policy does allow students to have personally owned mobile phones/ mobile devices within the Academy, do students know what the rules are for how and when they can be used? No
What are the sanctions for misuse? N/A
If personally owned mobile phones are not permitted within the Academy, how is the policy enforced? Staff to refer to sanctions matrix, and policy guidance. If children have personal devices, staff should confiscate temporarily and inform parents/carers immediately.
Are students made aware of the new forms of service and content increasingly available via mobile phones, such as picture and video messaging, Bluetooth, commercial content, and location-aware services, and the safety issues relating to these? Yes – Through computing curriculum
Are students made aware of how to protect themselves from mobile phone theft? Are they aware of procedures for reporting the IMEI (International Mobile Equipment Identity) number, hence disabling the phone if it is lost or stolen? Parents/Families and Children are aware to inform the school if personal devices are stolen, guidance on website for personal devices.
Are students aware how personally owned mobile phones and other personally owned devices can use in compliance with Oasis Off-site Activities and Educational Visits Policy? Yes, personal devices are prohibited.
Webcams
Are webcams used within the Academy for curriculum activities such as video conferencing? If so, are students aware of the appropriate behaviours to adopt when using them? Yes, acceptable users policy.
Are students aware of the issues of using webcams outside the Academy, such as inappropriate contact and Trojan horses which might activate a webcam without their knowledge? Yes through e-safety in the computing curriculum.

Peer-to-peer networks
Is access to peer-to-peer services required for student use and therefore permitted within the Academy? No
If not, are such services appropriately blocked on the Academy's network? Yes
Are students aware of the safety issues relating to peer-to-peer networks? Yes – e-safety within the computing curriculum.
Are students fully aware of the risks of viruses, and of the need to virus-check any materials downloaded and install firewalls to protect their own machines? Yes – e-safety within the computing curriculum.
Are students aware of their responsibilities with regards to illegally downloading or uploading materials to peer-to-peer networks? Yes – e-safety within the computing curriculum.
Third party supplied websites
Has the Academy identified the appropriate levels of privacy on personal data contained within third- party sites, and has guidance been distributed to staff, students and parents/carers in accordance with the OCL Data Protection Policy – Yes
Are systems in place to ensure the ethical use of data collected? - Yes – Policies
Are systems in place to ensure the validity of the information contained within the third-party site? – Unknown
Does the Academy have/require a 'gatekeeper' for third-party sites such as the role of Data Protection Lead? Yes – Matt

Academy procedures for Incidents, escalation points and sanctions

Levels matrix of acceptable and unacceptable use

An Academy must make decisions about specific use for some technologies which can be beneficial to learning. The table already indicates national policy for unacceptable use

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					X
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X

Adult material that potentially breaches the Obscene Publications Act					X
Criminally racist material in the UK					X
Pornography				X	
Promotion of any kind of discrimination				X	
Promotion of racist hatred				X	
Threatening behaviour, including promotion of physical violence or mental harm				X	
Any other information which may be offensive to colleagues or breaches of integrity of the ethos of Oasis or brings Oasis into disrepute				X	

Using Oasis systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Oasis IT Services section and/or Oasis				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Creating or propagating computer viruses or harmful files				X	
Carrying out sustained or instantaneous high-volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet and/or network				X	
Receipt or transmission of materials that infringe the copyright of another person or infringes the Data Protection Act				X	
On-line gambling				X	
On-line gaming (educational) – Academy decision		x			
On-line gaming (non-educational) - Academy decision				x	
On-line shopping/commerce - Academy decision		x			
File sharing - Academy decision		x			
Use of social network sites - Academy decision		x			
Use of video broadcast sites, e.g. YouTube, Vimeo - Academy decision		x			

Sanctions Matrix

These are sanctions that an Academy is required to decide how to deal with in terms of priority & hierarchy within an academy.

	Refer to class teacher / tutor	Refer to Head of Dept. / Head of Year / Other	Refer to Principal	Refer to Police	Refer to technical support team	Inform parents / carers	Removal of network / internet rights for fixed period of time	Warning	Further sanctions e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal	x	x	x	x		x	x		
Unauthorised use of non-educational sites during lessons or websites not relevant to current learning								x	x
Unauthorised use of any personal device	x							x	x
Unauthorised use of social networking / instant messaging / personal email / chat rooms	x							x	x
Unauthorised downloading or uploading of files	x							x	x
Allowing others to access Oasis network by sharing user names and passwords	x				x	x			x
Attempting to access or accessing Oasis network using another student's account	x	x	x			x			x
Attempting to access or accessing Oasis network using the account of a member of staff	x	x	x			x			x
Corrupting or destroying the data of other users	x					x			x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x					x		x	x

Continued infringement of the above following previous warnings and sanctions	x	x	x	x					
Actions which could bring Oasis into disrepute or breach the integrity of the ethos of Oasis	x	x	x						
Using proxy sites or other means to subvert the network filtering system	x				x		x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x		x		x			x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x						x
Receipt or transmission of materials that infringe copyright of another person or infringes the Data Protection Act	x				x				

Academy decisions re use of communication technologies

An Academy must provide explanations to support any contentious areas of use. The table already contains information about nationally agreed restrictions.

	Staff and other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Academy policy allows students to have personally owned mobile phones/mobile devices with them in school		x						x
Academy policy supports the use of mobile phones in lessons				x				x
Academy policy supports the use of mobile phones in social time	x							x
Taking photos on devices with inbuilt cameras		x					x	
Use of personal email addresses in Academy or on Academy network		x						x
Use of chat rooms / facilities				x				x

Use of instant messaging (e.g. Skype for Business, Yammer, iMessage, Messenger, Instagram etc.)	x					x		
Use of social networking sites		x						x
Use of blogs		x				x		
Use of devices provided by Oasis during lessons	x				x			
Use of personally owned devices during lessons				x				x

Appendix 4 – Reference - Roles and Responsibilities

1 Oasis Community Learning Group Executive

Aspect	Check
Has responsibility for ensuring that the Oasis E-Safety Policy is implemented across Oasis according to the terms within the policy	x
Are responsible for the approval of policies and guidance documents relating to the use of personally owned learning devices within the Academies	x
Has a named individual as the single point of contact for E-Safety issues within Oasis and with National agencies	x
Reviews the E-Safety Policy with advice from the National/Regional Oasis Directors, Academy Safeguarding Officers and the Head of Group IT Services	x

2 Regional Directors

Aspect	Check
Are responsible for ensuring and reviewing the effectiveness of the policy within an Academy with the Academy Council	x
Are responsible for approving high risk activities that are undertaken within an academy.	x
Will receive regular information about E-Safety incidents and monitoring reports for the Academies where they hold responsibility	x

3 Oasis Academy Principals, ALT, Academy DSL and Academy Data Protection Lead

Aspect	Check
Are responsible for the day to day implementation of the policies and guidance documents relating to the use of both Oasis equipment and personally owned devices within Oasis	x
Are responsible for updating and maintaining an effective Academy Operational ESafety Document	x
Will maintain an up to date Risk Register, analyse and evaluate the mitigation for events should they occur	

Will ensure that staff, students and other organisations working with Oasis are aware of the policies and guidance documents	x
Will ensure that staff, students, parents/carers all receive suitable opportunities for training in E- Safety. Where a person holds a role with responsibility, they have sufficient knowledge and expertise to carry out their role effectively.	x
Will receive regular information about E-Safety incidents and monitoring reports	x
Will request and regularly monitor the effectiveness of the filtering and change control logs	x
Will ensure that all staff, external agency personnel and students, have understood and agreed to the relevant Acceptable User Agreement	X
Will ensure that parents/carers have access to the Oasis E-Safety and Academy Operational E-Safety Policies	X
Will ensure that all parents/carers have access to the Acceptable User Agreement that their child will be required to agree with prior to having access to the Oasis IT systems	x
Will ensure that the Incidents and misuse matrices is adhered to by all users.	x

4 Oasis National/Regional, Cluster IT Support Teams

Aspect	Check
Will ensure that Oasis infrastructure is secure and is not open to misuse or malicious attack.	x
Will ensure that all Oasis-owned student devices will have E-Safety software installed. Internet access for any device on the Oasis network is provided through the Oasis filtering system.	x
Will ensure that users may only access Oasis's network through an enforced password protection policy in which passwords are required to the agreed IT Managed Service Level Agreement	x
Will provide access to educational resources, websites and online tools as authorised by Academy staff according to an agreed schedule of development/change control	x
Will ensure that they keep up to date with E-Safety technical information to effectively carry out their role and inform and update others as relevant	x
Will make sure that all aspects of the user experience, for example network, any Oasis Microsoft Office 365 and tools remote access, email are regularly monitored in order that any misuse/attempted misuse can be reported to Oasis	x
Ensure that the monitoring software systems are implemented and updated according to Oasis policies	x

5 Oasis staff, including external agencies (e.g. contractors/supply/ data processing) staff

Aspect	Check
Have access to see the full Acceptable User Agreement and have clicked online agreement statement to uphold the Acceptable User Agreement as relevant to their role and responsibilities.	X

Are responsible for ensuring that they have an up to date awareness of current ESafety matters according to the Oasis Acceptable Use for Technologies Policy and the current Academy policies such as the Use of Personally Owned Devices Policy	X
Report any incidents of misuse of the network systems or personally owned devices according to the agreed discipline procedures set out in the incidents and misuse matrices.	X
Carry out any digital communications with students on a professional level and only carried out using official Academy systems.	X
Embed E-Safety procedures into all aspects of their role within Oasis including curriculum and administration tasks alongside all other Academy activities	x
Ensure that all students follow E-Safety policies and guidance whilst in their care	X
Monitor tasks and activities using personal learning devices in lessons, extracurricular activities and any activities within extended Academy provision	X

6 Oasis students

Aspect	Check
Have clicked online agreement statement to uphold the Acceptable User Agreement.	X
Are aware and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.	X
Understand the importance of adopting good E-Safety practice when using digital technologies out of Academy and realise that Oasis's E-Safety policy covers their actions using personal learning devices outside of the Academy	X
Understand Oasis policy on taking images	X
Know the implications of and how to avoid cyber bullying and understand that this forms part of the Acceptable Use Agreement that they have signed.	X

7 Parents/Carers - All aspects need re-actioning in light of Covid-19 and future Horizons Project.

Aspect	Check
Have received a copy of the Acceptable User Agreement that is relevant to their child's access to the Oasis Community Learning IT systems, including Internet and email	x
Where relevant, have signed a Home Use Agreement for any Oasis owned equipment that is provided for their child to use	X
Be aware and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.	x
Understand the importance of adopting good E-Safety practice when using digital technologies and realise that Oasis's E-Safety policy covers their child's actions using Oasis Community Learning IT systems on personal learning devices outside of the Academy	x

Understand that Oasis has a specific policy on taking images and understand the implications of breaching this policy	X
Know the implications of and how to avoid cyber bullying and understand that this forms part of the Acceptable Use Agreement that they have signed.	x
Appreciate that according to the Acceptable User Agreement they could be held liable for any misuse of a personal learning device outside of Oasis	x

Appendix 4 Roles and Responsibilities

4.1 OASIS TRUST GROUP EXECUTIVE

- Has responsibility for ensuring that the Oasis E-Safety Policy is implemented across Oasis according to the terms within the policy
- Are responsible for the approval of policies and guidance documents relating to the use of personally owned learning devices within the Academies
- Has a named individual as the single point of contact for E-Safety issues within Oasis and with National agencies
- Reviews the E-Safety Policy with advice from the National/Regional Oasis Directors, Academy Safeguarding Officers and the Head of Group IT Services

4.2 NATIONAL/REGIONAL DIRECTORS / DATA PROTECTION OFFICER

- Are responsible for ensuring and reviewing the effectiveness of the policy within an Academy with the Academy Council
- Will receive regular information about E-Safety incidents and monitoring reports for the Academies where they hold responsibility

4.3 OASIS NATIONAL, REGIONAL, SITE-BASED IT SUPPORT TEAMS

- Will ensure that Oasis infrastructure is secure and is not open to misuse or malicious attack.
- Will ensure that all Oasis-owned student devices will have E-Safety software installed. Internet access for any device on the Oasis network is provided through the Oasis filtering system.
- Will ensure that users may only access Oasis's network through an enforced password protection policy in which passwords are required to the agreed IT Managed Service Level Agreement
- Will provide access to educational resources, websites and online tools as authorised by Academy staff according to an agreed schedule of development/change control
- Will ensure that they keep up to date with E-Safety technical information to effectively carry out their role and inform and update others as relevant
- Will make sure that all aspects of the user experience, for example network, any Oasis Microsoft Office 365 and tools remote access, email are regularly monitored in order that any misuse/attempted misuse can be reported to Oasis
- Ensure that the monitoring software systems are implemented and updated according to Oasis

policies

4.4 OASIS ACADEMY PRINCIPALS, ALT, DSL AND DATA PROTECTION LEAD

- Are responsible for the day to day implementation of the policies and guidance documents relating to the use of both Oasis equipment and personally owned devices within Oasis
- Are responsible for updating and maintaining an effective Academy Operational E-Safety Document
- Will maintain an up to date Risk Register, analyse and evaluate the mitigation for events should they occur
- Will ensure that staff, students and other organisations working with Oasis are aware of the policies and guidance documents
- Will ensure that staff, students, parents/carers all receive suitable opportunities for training in E-Safety. Where a person holds a role with responsibility, they have sufficient knowledge and expertise to carry out their role effectively.
- Will receive regular information about E-Safety incidents and monitoring reports
- Will request and regularly monitor the effectiveness of the filtering and change control logs

- Will ensure that all staff, external agency personnel and students, have understood and agreed to the relevant Acceptable User Agreement
- Will ensure that parents/carers have access to the Oasis E-Safety and Academy Operational E-Safety Policies
- Will ensure that all parents/carers have access to the Acceptable User Agreement that their child will be required to agree with prior to having access to the Oasis IT systems
- Will ensure that the Incidents and misuse matrices is adhered to by all users.

NB: An academy should ensure the following statements are correct within the academy and include within the training and support sessions

4.5 OASIS STAFF, INCLUDING EXTERNAL AGENCIES WORKING IN OCL

- Have access to see the full Acceptable User Agreement and have clicked online agreement statement to uphold the Acceptable User Agreement as relevant to their role and responsibilities.
- Are responsible for ensuring that they have an up to date awareness of current E-Safety matters according to the Oasis Acceptable Use for Technologies Policy and the current Academy policies such as the Use of Personally Owned Devices Policy
- Report any incidents of misuse of the network systems or personally owned devices according to the agreed discipline procedures set out in the incidents and misuse matrices.
- Carry out any digital communications with students on a professional level and only carried out using official Academy systems.
- Embed E-Safety procedures into all aspects of their role within Oasis including curriculum and administration tasks alongside all other Academy activities
- Ensure that all students follow E-Safety policies and guidance whilst in their care
- Monitor tasks and activities using personal learning devices in lessons, extracurricular activities and any activities within extended Academy provision

4.6 OASIS STUDENTS

- Have clicked online agreement statement to uphold the Acceptable User Agreement.
- Are aware and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good E-Safety practice when using digital technologies out of Academy and realise that Oasis's E-Safety policy covers their actions using personal learning devices outside of the Academy
- Understand Oasis policy on taking images
- Know the implications of and how to avoid cyber bullying and understand that this forms part of the Acceptable Use Agreement that they have signed.

4.7 PARENTS / CARERS

- Have received a copy of the Acceptable User Agreement that is relevant to their child's access to the Oasis Community Learning IT systems, including Internet and email
- Where relevant, have signed a Home Use Agreement for any Oasis owned equipment that is provided for their child to use
- Be aware and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Understand the importance of adopting good E-Safety practice when using digital technologies and realise that Oasis's E-Safety policy covers their child's actions using Oasis Community Learning IT systems on personal learning devices outside of the Academy
- Understand that Oasis has a specific policy on taking images and understand the implications of breaching this policy
- Know the implications of and how to avoid cyber bullying and understand that this forms part of the Acceptable Use Agreement that they have signed.
- Appreciate that according to the Acceptable User Agreement they could be held liable for any misuse of a personal learning device outside of Oasis

Appendix 5 – Reference - Acceptable Use of Technology Agreements

5.1 Terms and Conditions – Acceptable use of Technology Agreement Oasis Staff & Volunteers (including Academy Councillors and guests)

These are the Terms and Conditions for the Acceptable Use Agreement and are intended to ensure that:

- ✓ Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- ✓ Oasis IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- ✓ Staff are protected from potential risk in their use of IT in their everyday work.

Oasis will try to ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for student learning and will, in return, expect staff and volunteers to agree to be responsible and accountable users:

- ✓ I understand that I must use Oasis IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.
- ✓ I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT.
- ✓ I will, where possible, educate the students in my care in the safe use of IT and embed E-Safety in my work with students.

For my professional and personal safety:

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

I will be professional in my communications and actions when using Oasis IT systems: ✓ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- ✓ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ✓ I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with Oasis policy on the use of digital / video images. I will not use my personal

equipment to record these images, unless I have permission to do so. Where these images are published (e.g. Microsoft Office 365 and tools) it will not be possible to identify by name, or other personal information, those who are featured.

- ✓ I will only use chat and social networking sites in Oasis in accordance with the Oasis policies.
- ✓ I will only communicate with students and parents / carers using official Oasis systems. Any such communication will be professional in tone and manner.

- ✓ I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- ✓ When I use personally owned devices (e.g. hand held / external devices- PDAs / laptops / mobile phones / USB devices etc.) in Oasis, I will follow the rules set out in this agreement, in the same way as if I was using Oasis equipment. I will comply to the Oasis Use of Personally Owned Devices Policy (UPOD)
- ✓ I will not use personal email addresses on the Oasis IT systems.
- ✓ I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- ✓ I will ensure that my data is saved on the Oasis network and where this is not possible that it is backed up, in accordance with relevant Oasis policies.
- ✓ I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), inappropriate or may cause harm or distress to others.
- ✓ I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to inappropriate materials.
- ✓ I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- ✓ I will not install or attempt to install programmes of any type on a device, or store programmes on a device, nor will I try to alter computer settings, unless allowed within my Oasis role and level of permissions.
- ✓ I will not disable or cause any damage to Oasis equipment, or equipment belonging to others.
- ✓ I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Oasis Data Protection and Information Security Policies (or other relevant Oasis policy). Where personal data is transferred outside the secure Oasis network, it must be encrypted.
- ✓ I understand that Oasis Data Protection and Information Security Policies require that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Oasis policy to disclose such information to an appropriate authority.
- ✓ I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

5.2 Terms and Conditions – Acceptable Use of Technologies Agreement – Oasis Primary Key Stage 2 students

You are going to use Oasis IT systems and equipment to make it easier to work in Oasis or at home.

To make sure that you can work safely we need you to keep to some rules. You must read them carefully and understand what they mean.

Starting Off:

I know:

- ✓ I must agree to these rules
- ✓ I will be in trouble if I do not follow them. My teachers might stop me using the IT systems and equipment
- ✓ I am responsible for my own user space **AND** anything unsuitable found there is my responsibility;

I will:

- ✓ make sure that any contact I make with others on the Oasis system is responsible, polite and sensible;
- ✓ only use my Oasis email address for emails
- ✓ only upload materials which are free from copyright and suitable for Academy use;
- ✓ be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe;
- ✓ treat all IT equipment with care;
- ✓ only use devices with permission from my teachers;
- ✓ keep my password safe and tell a teacher if someone else knows my password;
- ✓ report and discuss anything I am worried or concerned about on the Oasis system with my teacher
- ✓ only use the access to resources given by my teachers;

(The following section may be removed if personal devices are not provided by Oasis for student personal use in and outside of the Academy) When I am given my own Oasis device to use I will:

- ✓ *look after my Oasis device very carefully all the time*
- ✓ *ensure that it is charged every evening if I have taken it home to use so that it is ready for use the next day;*
- ✓ *bring my Oasis device to the Academy every day, unless I have been told not to;*
- ✓ *make sure my Oasis device is kept in the secure storage area always when not in use at Oasis;*
- ✓ *take care when my Oasis device is transported that it is as secure as possible (e.g. not left visible in a vehicle; not left unattended on a bus);*
- ✓ *make sure the device is not damaged by any play activities (like running with it around the playground, pushing others in a queue)*
- ✓ *take care to stop any computer viruses infecting my Oasis device. If I am not sure, I will talk to a teacher **BEFORE** connecting it to Oasis network;*
- ✓ *not decorate the device or its case and not allow it to be subject to graffiti.*

If I can use personally owned devices in the Academy:

- ✓ I know that this Agreement covers the use of my personally owned devices with any Oasis system both inside and outside of an Academy
- ✓ I am responsible for the safety of my personally owned devices, Oasis is not responsible for the loss or theft of a device, nor are they responsible for any damage done to the device while at school;
 - ✓ I will use an approved device
- ✓ My personally owned device will only be used for an educational reason, and in class only use it when given permission to do so by the teacher
- ✓ I must keep my personally owned devices turned off when not using them;

- ✓ I may not use my personally owned device camera to capture, record, or transmit audio, video or still photos of other students, or staff without explicit permission given by the subject of the photo or video;
- ✓ I must not use my personally owned device in a manner that is disruptive to the educational environment in the academy or allow it to disrupt other students;
- ✓ If I misuse my personally owned device for any form of cyber-bullying or inappropriate behaviour, I will be disciplined under OCL Bullying policy and procedures.
- ✓ I will act to prevent computer viruses on my personally owned devices. If in doubt that a virus is on my personally owned device, I will report the matter **BEFORE** connecting it to Oasis network;
- ✓ If I intend to use my personally owned device in school, I will ensure that it is charged every evening so that it is ready for use the next day;
- ✓ I am responsible for servicing of my personal electronic devices. Oasis will not service, repair or maintain any non-Oasis owned technology brought to and used at school by students.

I will not:

- x share my username, password or personal information with anyone else
- x look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this, I will tell a teacher
- x deliberately misuse or deface another users' work on the Oasis network.
- x access or try to access any illegal material;
- x download files without permission;
- x get around or try to get around the Oasis network security measures
- x use or amend images or text that may cause distress or offence;
- x bring material into Oasis that has not been virus checked;
- x use Microsoft Office 365 and tools or email to share/distribute files or information that is illegal, of adult content or may cause offence or distress;
- x without permission, plug in or unplug any computer cables or accessories at any time including the device provided by Oasis or my personally owned devices including mobiles phones;
- x log into the network / internet / log into the network / internet / Microsoft Office 365, or email with a user name or password that is not my own;
- x use another person's account at any time;
- x intentionally misuse Oasis blogs, Oasis Instant Messaging (Skype for Business) or Oasis accounts;
- x access or try to access chat rooms, forums, messaging, social networking or sites with gambling or adult content;
- x use IT equipment for fraudulent purposes;
- x deliberately damage the computer equipment or use the network in a manner that will prevent other using it.

Oasis will:

- ✓ monitor your use of the Internet and may take further action if a member of Oasis staff is concerned about your safety
- ✓ check your user area regularly to ensure correct and appropriate usage;
- ✓ make sure that you are using the facilities responsibly and in an appropriate manner;
- ✓ be able to delete any material in your user area that is not coursework / classwork, at any time, without warning;

If you disobey any of these rules it:

- ✓ will result in a temporary or permanent ban of Internet and/or network;
- ✓ may result in additional disciplinary action in line with existing practice on inappropriate behaviour;
- ✓ may lead to involving your parent(s) / carer or the police.

5.3 Terms and Conditions - Acceptable Use of Technologies Agreement - Secondary Students

Oasis recognises that to enhance their learning, students are required to use a wide range of technologies including computers, the network and the Internet.

As a student at an Oasis Academy you are being provided with access to Oasis IT systems and equipment. We must make sure that you will be as safe as possible when using any of the technologies provided by Oasis and have created some simple rules that will apply to all students.

You are responsible and accountable for your own use of technologies, but by sticking to these rules we believe that you will be working within as safe a learning we can possibly provide for you.

Before you can begin to use technologies within Oasis Academy you have to:

- ✓ Agree online that you to this Acceptable Use Policy before access to the Oasis systems is allowed
- ✓ Accept that you will be required to read, and abide by a contract of use should you disobey any of Internet or network rules **before** being given access again;

To keep yourself safe you agree that you WILL:

- ✓ Only use the computers to enhance your own learning;
- ✓ Only use your Oasis email address for communication
- ✓ Treat the ICT equipment with care;
- ✓ Use your time on the computers effectively;
- ✓ Keep your password safe and report any password that someone else knows;
- ✓ Only store coursework / classwork in your user area
- ✓ Report and discuss any concerns and **ALL** violations witnessed with class teacher
- ✓ Only use approved access to resources (such as a Twitter feed) as provided by your teachers;

(The following section can be removed if personal devices are not being provided by OCL)

- ✓ *look after my Oasis device that I have been given very carefully all of the time and ensure that it is charged every evening, ready for use the next day;*
- ✓ *bring my Oasis device to Academy every day, unless I have been told not to;*
- ✓ *make sure my Oasis device is kept in the secure storage area at all times when not in use at Oasis;*
- ✓ *take care when my Oasis device is transported that it is as secure as possible (e.g. not left visible in a vehicle; not left unattended on a bus);*
- ✓ *make sure my Oasis device is not subject to careless or malicious damage (e.g. because of horseplay);*
- ✓ *take reasonable precautions to prevent the introduction of computer viruses. If in any doubt whether a virus has contaminated my Oasis device, I will report the matter **BEFORE** connecting it to Oasis network;*
- ✓ *not decorate my Oasis device or its case and not allow it to be subject to graffiti.*

When the Academy allows the use of personally owned devices:

Using your personally owned devices in school:

- ✓ I know that this Agreement covers the use of my personally owned devices with any Oasis IT system both inside and outside of an academy site
- ✓ I am responsible for the safety of my personally owned devices, Oasis is not responsible for the loss or theft of a device, nor are they responsible for any damage done to the device while at the Academy;
- ✓ I will use an approved device
- ✓ I will use my personally owned device for an educational reason, and in class only use it when given permission to do so by the teacher

- ✓ I must keep my personally owned devices turned off when not using them;
- ✓ I may not use my personally owned device camera to capture, record, or transmit audio, video or still photos of other students, or staff without explicit permission given by the subject of the photo or video;
- ✓ I must not use my personally owned devices in a manner that is disruptive to the educational environment in the academy or allow it to disrupt other students;
- ✓ If my personally owned devices are used for any form of cyber bullying or intimidating behaviour, I will be disciplined under Oasis Bullying policy and procedures.
- ✓ I will act to prevent computer viruses. If in any doubt whether a virus has contaminated my personally owned devices, I will report the matter **BEFORE** connecting it to Oasis network;
- ✓ If I intend to use my personally owned devices in school, I will ensure that they are charged every evening ready for use the next day;
- ✓ I am responsible for servicing of my personally owned devices. Oasis Community Learning will not service, repair or maintain any non-Oasis owned technology brought to and used at school by students.

To protect yourself you agree that you WILL NOT:

- × access or try to access any illegal material;
- × download non-coursework/classwork files without permission;
- × use material for classwork / coursework without permission from the copyright holder / owner;
- × actively bypass Oasis security measures including the use of proxy bypass websites;
- × use or amend images or text that may cause distress or offence;
- × bring material into Oasis that has not been virus checked;
- × use any ICT equipment to harass, bully, abuse or otherwise distress any individual inside or outside Oasis;
- × use Oasis 365 environment/email to share/distribute files or information that is illegal, of adult content or may cause offence or distress;
- × without permission, plug in or unplug any computer cables or accessories at any time including the device provided by Oasis or personally owned mobiles phones;
- × log into the network / internet / Microsoft Office 365 and tools, or email with a user name or password that is not your own;
- × use another person's account at any time;
- × store files on your user area that are not related to classwork or coursework;
- × use ICT equipment / Internet for recreational use in Oasis without permission from a member of staff;
- × access or try to access chat rooms, forums, messaging, social networking or sites with gambling or adult content;
- × use ICT equipment for fraudulent purposes;
- × use images or information on weapons and/ or drugs at any time unless specifically for coursework/classwork;
- × use ICT equipment to buy goods online;
- × deliberately damage the computer equipment or use the network in a manner that will prevent other using it.

To make sure the learning environment stays safe, you need to know that:

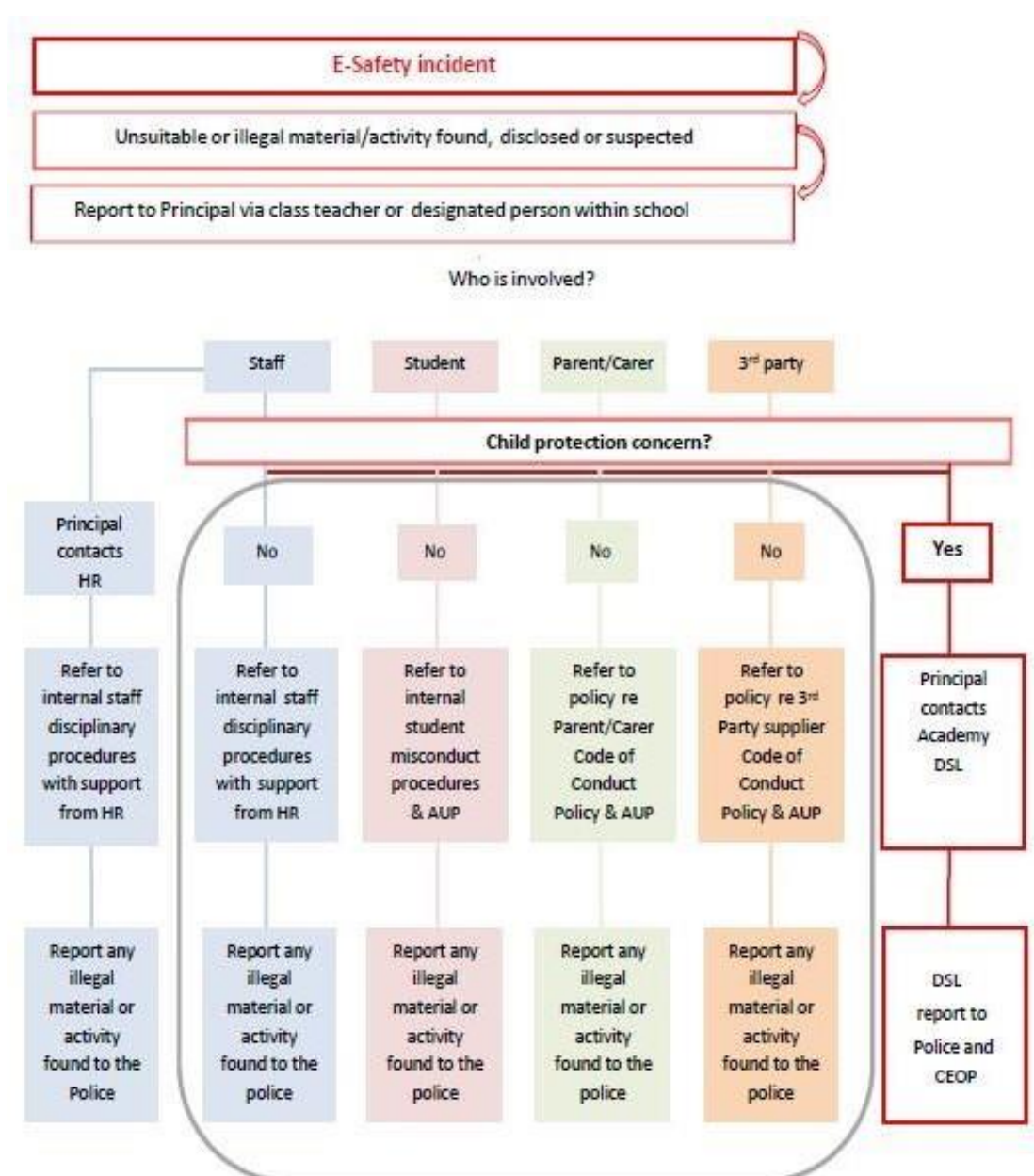
- ✓ Oasis will be checking your user area regularly to ensure correct and appropriate usage;
- ✓ you have a responsibility to use the facilities in an appropriate manner;
- ✓ you are totally responsible for your own user space **AND** any unsuitable material found in your user area is your responsibility;
- ✓ any material in your user area that is not coursework / classwork could be deleted at any time, without warning;

- ✓ you are advised not to use social networking sites to maintain contact with staff including having them as friends. Students choosing to ignore this advice may be subject to disciplinary proceedings in the event of a case being proven.

And if you did disobey any of these rules it:

- ✓ will result in a temporary or permanent ban of Internet and/or network;
- ✓ may result in additional disciplinary action in line with existing practice on inappropriate behaviour;
- ✓ may lead to involving your parent(s) / carer or the police.






Appendix 6 – Reference - Flow Diagram E-Safety incident reporting



Appendix 7 – Guidance - Age appropriate agreement discussion & Rules for Students

Discussion Posters Key Stage 1

SMARTthinking

<p>S</p>	<p>Safe</p>  <p>STOP and THINK Will the information you share keep you safe?</p>
<p>M</p>	<p>Meeting</p>  <p>STOP and THINK Are your online friends who they say they are?</p>
<p>A</p>	<p>Accepting</p>  <p>STOP and THINK How do you know files and pictures are safe?</p>
<p>R</p>	<p>Reliable</p>  <p>STOP and THINK How do you know that people or pages aren't lying?</p>
<p>T</p>	<p>Tell</p>  <p>STOP and THINK Who can you tell if you feel uncomfortable about something online?</p>

Our eSafety Top Tips!

1

People
you don't know
are strangers.

They're not
always who they
say they are.



2

Be nice to
people
like you
would
on the
playground.



3

Keep your personal
information private.



4

If you ever
get that
'uh oh'
feeling,
tell a grown-up
you trust.



Rules for Students

To be adapted or adopted by an Academy and displayed where users are accessing online Oasis system and Microsoft Office 365 or the internet.

SAFETY FIRST

Information is power!

- ✓ Keep personal information, password and data safe by ensuring that it is not shared with others.
- ✓ Only access Oasis's network using user account and password, ✓ Do not give user name and password to anyone else.
- ✓ If you think someone has learned your password, inform a member of staff immediately. ✓ Log off after having finished using the computer.
- ✓ If you find a machine logged on under another user's account, inform a member of staff who will ensure that the machine is safely shut down.

Respect!

- ✓ Show self-respect through your actions. Only use appropriate language and images both within the Learning Platform and on the internet.
- ✓ Do not post inappropriate personal information about your life, experiences or relationships.
- ✓ Do not use any electronic mediums to bully, harass or stalk people.
- ✓ Do not visit any websites that are degrading, pornographic, racist or that Oasis would deem inappropriate
- ✓ Do not abuse access privileges by attempting to or entering other people's private spaces or work areas.

Protect!

- ✓ Ensure that information posted online will put no-one at risk, including you.
- ✓ Do not publish full contact details, a schedule of activities, or inappropriate personal details in public spaces.
- ✓ Report any aggressive or inappropriate behaviour directed at anyone, including you.
- ✓ Do not forward, save or print materials (including emails and images) that Oasis would deem inappropriate or that may cause offence to others.

Appendix 8 – Guidance - Use of technologies around Oasis Academies

As new technologies emerge and students become more autonomous learners it is important to develop a protocol for the use of personal learning devices in and around the Academy environment.

These tables illustrate behaviours relative to the use of technologies in a typical Academy day where students have access to personal devices either provided by Oasis or personally owned. A key factor in establishing how personally owned devices (or any Oasis equipment) can be used is the level of autonomy against that which requires consent. The intention is to use these statements at ESafety meetings that are held regularly as a checklist/guide as to behaviours to be applied within individual academies and use them to support the [Operational E-Safety Manual \(Section 2.1 – Overview\)](#).

These scenarios illustrate a situation both where Oasis has provided the device and where academy policy permits users to bring their own devices into the Academy environment.

Student expectations for how they want, and are able, to use technologies to support independent learning are high and demand is likely to increase. Therefore, it is advisable to devise an Academy strategy to manage these expectations.

Matching the agreed protocol for use with the Academy sanctions policy and the signed Acceptable Use Agreements would complete the picture. Please see samples of these level documents included in this Appendix.

Before the Academy day starts
<i>Students are expected to:</i>
Bring any personal device permitted by academy policy into Oasis that will be used within lessons every day unless told not to
Make sure that any device required has been charged ready for use throughout the day in Oasis.
Keep any personal device permitted by academy policy in their bags until they are within a classroom or 'safe' approved area within Academy grounds.
Make sure any personal device permitted by academy policy is not damaged by any play activities (like running with it around the playground, pushing others in a queue).
<i>Staff, Teachers, TA and External Agency personnel are expected to:</i>
Ensure that the students are complying with the Student Acceptable Use Agreement and, if any misconduct is identified, apply the correct level of discipline/sanction.

During lessons
<i>Students are expected to:</i>
Make sure that whatever they do is in compliance with the Student Acceptable Use Agreement that they have agreed.
Report any concerns that any device they are using might have been exposed to computer viruses to a teacher before connecting it to Oasis network.
Report any technical difficulties with Oasis equipment directly to their teachers.
Ask permission before they plug in or unplug any computer cables or accessories at any time including the device provided by Academy or any personal device permitted by academy policy.
<i>Staff, Teachers, TA and External Agency personnel are expected to:</i>
Ensure that the students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.
Ensure that any technical issues relating to the use of the devices is reported to a class teacher in the first instance who will establish the details before reporting to the local IT Service team via the Service Desk system, through a form on the online Oasis systems and Microsoft Office 365, or by email

During assemblies and lessons where devices will not be used
<i>Students are expected to:</i>
Store any devices used in a safe secure storage space as allocated to them

Make sure any personal device permitted by academy policy is not damaged by any play activities (like running with it around the playground, pushing others in a queue).
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure that the students are complying with the Student Acceptable Use Agreement) and if any misconduct is identified apply the correct level of discipline/sanction.

During breaks and lunch

<i>Students are expected to:</i>
Make sure any personal device permitted by academy policy is not damaged by any play activities (like running with it around the playground, pushing others in a queue).
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure that the students are complying with the Student Acceptable Use Agreement) and if any misconduct is identified apply the correct level of discipline/sanction.

After the Academy day finishes

<i>Students are expected to:</i>
Make sure any device is not damaged by any play activities (like running with it around the playground, pushing others in a queue).
Staff, Teachers, TA and External Agency personnel are expected to:
If devices re being used within clubs or after the Academy activities the same protocol as for lessons is to be followed.
Ensure that the students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.
Ensure that any technical issues relating to the use of the devices is reported to a class teacher in the first instance who will establish the details before reporting to the local IT team via the Service Desk system, through a form on online Oasis systems and Microsoft Office 365, or by email.

In remote locations, including home environment, work placements, colleges

<i>Students are expected to:</i>
Ensure that any device required is charged every evening, ready for use the next day within the remote location (where this is not their home environment).
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure that the students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.
Parents /carers are expected to:
Ensure that the use of any Oasis owned device is in compliance with the Home Use Agreement.

During transportation

<i>Students are expected to:</i>
Carefully transport any Oasis owned devices in the carry case provided
Make sure that when any Oasis owned device is transported it is as secure as possible (e.g. not left visible in a vehicle; not left unattended on a bus).

<i>Staff, Teachers, TA and External Agency personnel are expected to:</i>
Ensure that the students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.
<i>Parents /carers are expected to:</i>
Ensure that the use of any Oasis owned device is compliant with the Home Use Agreement.

Appendix 9 – Guidance - Sample Home Use Agreement - Oasis equipment

Home / Academy Agreement - Oasis provide a device for personal use

To help ensure that your child a student at Oasis Academy

the principles outlined in this agreement. As an Academy we are prepared to provide all the back-up and resources required for the Oasis owned device to work but we also need the commitment of both parents/carers and students.

As you read through the document you will see a summary of the e-learning commitment that the Academy is making to the students. It also outlines the commitment we need from the home and from the students themselves.

When you have read the document, we invite you and your child to sign this agreement and return it to the Academy. This will ensure that we are all working together to ensure success

The Academy will:

- ☐ Arrange for a device to be available for your child to use

At Home we will:

- Ensure that our child understands how to care for and protect their device in the home environment.
- Report any loss or damage promptly, including accidental loss or damage
- Report any faults in hardware or software promptly.
- Ensure that the device is returned at the end of the agreed time period or at any other time at the request of a member of Academy staff.
- Make sure that the device is not used for any illegal and/or ant-social purpose, including access to inappropriate internet sites and social networking sites, Apps and chat rooms
- Ensure our child follows the ideals below.

As a student I will:

- Look after my device very carefully all of the time and make sure that I charge it each evening ready for use in the Academy next day

Please sign and return to the Academy as soon as possible.

Student Agreement

I agree to abide by these terms in my use of the Oasis device.

Name:

Class:

Signed:

Date:

Parent/Carer Agreement



- ☐ for the length of this agreement.
Make sure the device is working and that repairs are dealt with as quickly as possible. Where repairs are not possible a replacement may not be available, so students will be encouraged to 'buddy-up' with others
- ☐ to allow learning to continue.
Make sure that the device is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss or damage.
- ☐ Provide a secure storage area where the device can be stored when it is not needed in a lesson.
- ☐ Ensure that the device is protected against computer viruses
- ☐ Provide parents/carers and students a comprehensive introduction to using and caring for the device and resources available
- ☐ Identify each device clearly so that students will be able to identify their own device easily.

- ☐ Bring the device in to the Academy every day unless I have been told not to
- ☐ Make sure my device is kept in the secure storage area at all times when not being used in the Academy
- ☐ Take care when I am transporting my device, so it is as secure as possible (e.g. not left visible in a vehicle, not left unattended on a bus)
- ☐ Make sure my device is not subject to careless or malicious damage (e.g. as a result of horseplay)
- ☐ Take precautions to prevent computer viruses and if in any doubt that my device is contaminated I will report the matter BEFORE connecting o the Academy network
- ☐ Not decorate my device or the case and not allow it to be subject to graffiti.

I agree to my child having the personal use of an Oasis device on these terms.

Signed:

Date:

Terms & Conditions:

Failure either to take such reasonable care or to abide by the conditions listed in this document (and the Acceptable Use of Technologies Agreement) may result in the device being reclaimed. The Academy also reserves the right to claim financial recompense in such cases.

If the device is used to connect to the internet at home, the Academy will **NOT** be responsible for any costs incurred. Additionally, the Academy cannot be held responsible for E-Safety within the home but will provide support to ensure the learning environment is as safe as possible. The device should be charged at home overnight, but the Academy cannot accept responsibility for electricity or internet costs.

The Academy will: XXXX can gain maximum benefit we invite you to agree to

(Note that permission to take Oasis equipment home will be contingent on this agreement being signed and amended for individual Academy requirements)

E-Safety Policy

(V9.2/ July 2018)

(IT Business Relationship Manager/ Review: November 2019)

Appendix 10 – Guidance - Developing safe use of Learning Technologies

To support the safe use of learning technologies Oasis IT Services have created a shared Microsoft Office Class Note Book.

The Class Note Book is available to all users and is to be updated on an annual basis to reflect the new and additional tools available through the Oasis IT System.

The resource contains an overview of the learning tools available through Oasis network and ideas about how to integrate them into teaching and learning.

The sections within the Note Book are:

- **Learning, Sharing Productivity Tools**
- **Creativity Tools**
- **Strategic Development and Tracking**
- **IT National Challenges**
- **Accreditation Routes**

Supporting Learning Technologies

Learning, Sharing and Productivity tools



Creativity tools



Strategic Development and Tracking



IT National Challenges 2017 - 2018



Accreditation Routes

Appendix 11 – Guidance - Oasis IT Frameworks for developing use of Learning Technologies

There are 3 related Oasis IT Services Frameworks that can be used to support Academy development of learning technologies:

- Readiness for Learning Technologies
- Identifying the Learning
- Outstanding Digital Learners

Readiness for Learning Technologies

This Framework is split into the following sections:

- Define your goals
- Define curriculum role
- Supporting devices for learning
- Planning CPD strategy
- Ensuring E-Safety
- Engagement strategy
- Promoting digital literacy

Each section contains a series of questions with different level of response available.

Action Point 1	Have you already chosen the range of devices that you would like to have accessible within your school environment?	Yes	Please complete 'Device range' pro-forma to indicate your choice of devices and share with your IT Support Team	Ready
Action Point 2	Do you require specific devices for some subject areas? For example, high quality video and digital images in Media/Photography, 3D printing facility within D&T.	Yes	Please complete the 'Subject Requirement' pro-forma with details of the subject areas where you require specialist devices and equipment available and share with the IT team	Ready
Action Point 3	Have you identified the range of software applications required needed to deliver the National Curriculum subjects that you are offering?	Some gaps	To help you make decisions please refer to the 'Software Catalogue' document to help you make your decisions and then complete the 'Software Library' pro-forma before sharing it with the IT Team.	Not yet ready
Action Point 4	Do you have any specialist software requirements for 16+, Community or external organisations that have access to your school system?	No	There are useful suggestions in the Extended School Software document if you should be considering offering wider access to community or older students	Not ready
Action Point 5	Do you expect to be using a range of Web 2 tools within teaching and learning environment?	Not sure	To identify relevant Web 2 tools please look at the 'Web 2 Tools for Learning' document and if there are relevant tools please complete the 'Web 2 Tools Requirements' pro-forma and share it with the IT Team.	Not yet ready
Action Point 6	Do have a list of recommended Apps (iPhone/iPad, Windows, Android) that you would like users to be able to access?	Not complete as yet	The 'Apps for Learning Catalogue' contains recommended Apps to assist you in identifying relevant Apps. When you have made your choices please complete the 'Apps for Learning Requirement' pro-forma and share with the IT Team	On the way

When completed a 'Readiness Report' is generated, this can provide the baseline data for the Action Research project.

Aspect 1: Define device role										Define device role	
Action Point 1	Action Point 2	Action Point 3	Action Point 4	Action Point 5	Action Point 6	Action Point 7	Action Point 8	Action Point 9	Action Point 10		
Please complete 'Device range' pro-forma to indicate your choice of devices and share with your IT Support Team	Please complete the 'Subject Requirement' pro-forma with details of the subject areas where you require specialist devices and equipment available and share with the IT team	To help you make decisions please refer to the 'Software Catalogue' document to help you make your decisions and then complete the 'Software Library' pro-forma before sharing it with the IT Team.	There are useful suggestions in the Extended School Software document if you should be considering offering wider access to community or older students	To identify relevant Web 2 tools please look at the 'Web 2 Tools for Learning' document and if there are relevant tools please complete the 'Web 2 Tools Requirements' pro-forma and share it with the IT Team	The 'Apps for Learning Catalogue' contains recommended Apps to assist you in identifying relevant Apps. When you have made your choices please complete the 'Apps for Learning Requirement' pro-forma and share with the IT Team	Please select response from drop down list and press enter	Please select response from drop down list and press Enter	Please select response from drop down list and press Enter	Please select response from drop down list and press Enter		
Readiness Level: Ready	Ready	Not yet ready	Not ready	Not yet ready	On the way					Overall readiness rating = 33%	

Identifying the Learning

This Framework enables a full curriculum mapping not only of what individual year groups and

classes

location of working.

The different nature of the learning that is taking place can be identified thus ensuring that there is a spread of experience and access to a range of tools and devices. For example, the use of the collaborative tools within Office 365 can provide an insight into student attitude, therefore planned sessions can be evaluated to see the impact upon behaviour, attitude and attainment.

This is primarily a planning tool to make sure that any learning technologies are available at the right time, in the right place and in the right amount, but also gives a guide for discussing future procurement and refresh requirements. The sections that provide the final mapping are:

- ❑ Curriculum mapping
- ❑ Learning attributes/pedagogy models
- ❑ Available technologies
- ❑ Year group / Users experience

The output from this framework can form the basis for a structured refresh / development plan in conjunction with staff CPD.

Year Groups		Connecting knowledge with learning	
Resource Base			RB
Nursery/Reception			NR
Year 1			Y1
Year 2			Y2
Year 3			Y3
Year 4			Y4
Year 5			Y5
Year 6			Y6

Framework Strands		Connecting experiences and learning	
2D-3D Design			DE
Program Technical			PT
Images			IM
Animation			AN
Audio			AU
Music			MU
Presentation			PR
Information			IN
Publication			PU
Research			RE

Constructive learning		Connecting doing with learning	
Demonstrating			D
Speaking			F
Making			M
Undoing			U
Inventing			I
Solving			S
Trialling			T

Laptop - PC Staff			CL
Laptop (Other, iBook etc)			LI
Tablet - (ipad or equivalent) Staff			TT
Desktop PC Student			DS
Laptop - PC Student			LS
Tablet (ipad or equivalent) Student			TS
Monitors			MO
Android			A
Personal device - mobile phone or equivalent used in class			PD
Digital cameras			DC
Graphic calculators			GC
Nintendo DS or equivalent			N
Video cameras			VC
Green screen			SS
Recording/broadcast system			RB
Music Keyboards			MK
Visualisers			VC
IWB			IWB
Fixed Projectors			PS
Mobile Projectors			MP
Web cam - either incorporated into tablets or laptops			WC
School Internet access			SI
Remote Internet access			RI
In school network access			SN
Remote Office 365 access			RN
In school access to purchased learning resources			SLR
Remote access to purchased learning resources			RLR
Laptop Trolleys			LT



Term 2 Timing TBC	History Focus Bristol Bombing - Use of online data and Google maps map a journey around Bristol for what it looked like then and now, placing images on Google etc.	Information Animation Images Presentation	Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information	Laptops iPads - accelerated reader sessions Digital Toolkits - camera, audio recorder, tripod, mini tablet device	42 Movie MovieMaker Photostory3 Purple Mash Audio App - Audacity Garage Band - iPads
	Geography What is a rock? project - time lapse and video clips of students experimenting with different types of rock and producing either / or / both Technical and Documentary videos based on Geology around Bristol and any linked impact during Bristol Bombing	Film Presentation Research Publication Audio Program / Technical	Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information Use sequence, selection, and repetition in programs; work with variables and various forms of input and output Design, write and debug programs that accomplish specific goals..... solve problems by decomposing them into smaller parts	Laptops iPads Digital Toolkits - camera, audio recorder, tripod, mini tablet device Lego Robot kit	42 Movie MovieMaker Photostory3 Purple Mash Audio App - Audacity Garage Band - iPads Ideas for research into geology; http://www.sciencekids.co.nz/geology/
Extras	<ul style="list-style-type: none"> Unpredictable access levels to the network / internet from within the room - some days can take 20 minutes to resolve the issues Same mismatch of versions of things on devices used by teachers students Need to know that students can access same Apps and websites, seem to be inconsistency between what 	Add in: 2D and 3D Design Music e-Safety Developmental logic Computational thinking	Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; Understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration	Laptops Digital Toolkits - camera, audio recorder, tripod, mini tablet device Control devices - sensors etc	Computational thinking / Developmen logic: https://eraseallkittens.com/en/play/ (works best on Chrome); https://code.org/ Sample problems and free courses (vic lesson plans etc); https://wrolearnin.com/straightfor

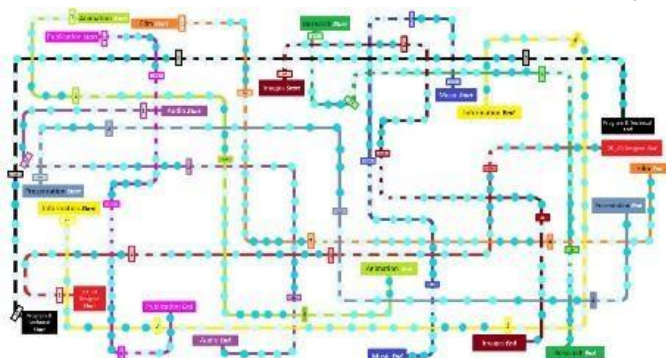
are planning to do at any time but also the resources devices and

Outstanding Digital Learners

The framework pulls together a student's viewpoint for incremental progress with the digital skills that they have identified as necessary for their personal development and want to be able to use effectively in their studies.

This has been created in conjunction with tracking progress and planning tools for staff. Each of the skills is split into levels relevant from the beginning of school years through to 16+ and cover Knowledge, Skills and Collaboration.

There is an interactive record of progress levels against each skill and an overall report. These can be used for accreditation within an Academy setting their own benchmarks for success. There is potential to look for accreditation through organisations such as Apple / Microsoft.

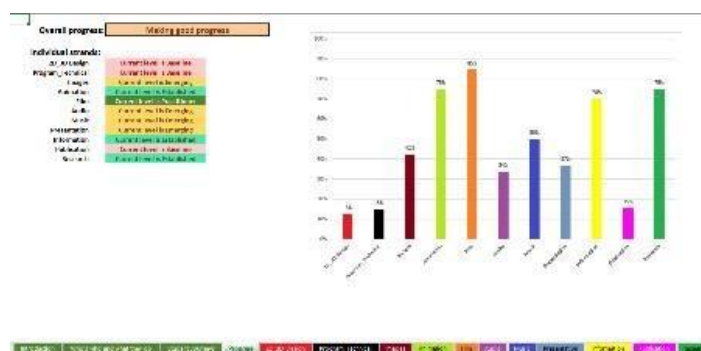


The digital skills (as identified by students) are:

- 2D & 3D Design
- Program_Technical
- Images
- Animation
- Film
- Audio □ Music
- Presentation
- Information
- Publication
- Research



Outcome will establish which key skills an individual considers essential and where and how these can be incorporated into a CPD strategy – for students, staff and potentially parents. The leadership role will have to include identifying potential for improving learning and who should have responsibilities for doing what in relation to these skills.



Appendix 12 – Guidance - E-Safety within other Oasis Policies

The overarching policy document, E-Safety Policy, has been developed to cover all aspects for the use of IT within Oasis. Following a review of the existing E-Safety policies it is apparent that some of the educational policies could benefit from more explicit reference to how technologies could and should be utilised within Oasis Academies.

Links have been cross-referenced from individual education policies to the main AOTP. In addition, as Appendices to the main policy document there are a series of guidance documents that an individual Academy could choose to adopt or adapt as they wish for their own requirements. References have been made to the Guidance documents as seems appropriate within the education policy documents.

Reference to aspects of E-Safety can be found within the following Oasis Policies:

- OCL Safeguarding
- Anti-bullying Policy
- Behaviour for learning Policy
- Curriculum Policy (Primary)
- Teaching and learning Policy & Guidance (Primary)
- Curriculum Policy (Secondary)
- Teaching and Learning Policy (Secondary)
- Parental/Carer's Code of Conduct Policy
- Offsite activities and educational visits Policy
- Oasis Data Protection Policy
- Oasis IT Security Policy
- Oasis Acceptable Use of Technologies Policy
- Oasis Use of Personally Owned Devices Policy (UPOD)

OCL Safeguarding

At Oasis Community Learning we strive to make sure all our students are safe in school, at home, on line and in the community. Our staff are here to keep young people safe and secure and to promote their personal safety and wellbeing.

Our commitment to safeguarding encompasses ways which we ensure children and young people foster security, confidence and independence. The Academy has a duty of care and the right to take reasonable action to ensure the welfare and safety of its pupils. If a member of staff has cause to be concerned that a child may be subject to ill treatment, neglect or any other form of abuse, the Academy will follow child protection procedures and inform Children's Services of its concern.

A clear policy on Safeguarding is available below and is reviewed by staff and the Academy Council on an annual basis.

There are designated lead staff who monitor the effectiveness of the policy and, where necessary, liaise with the local authority when significant safeguarding concerns arise.

If you have a concern that a child is being harmed, is at risk of harm, or you receive a disclosure (intentionally or unintentionally) you must contact one of the designated safeguarding leads as quickly as possible. You will find the names of these members of staff on the Academy's Safeguarding Policy.

Policy and Procedures

We will ensure all policies and procedures in respect of safeguarding children are up to date and in line with latest DfE legislation (www.gov.uk/government/publications/keeping-children-safe-in-education--2). The policies are accessible to all staff through the Oasis Zone and Academies Virtual Learning Environment (VLE). Policies and procedures are reviewed and revised by the Oasis Board of Trustees on a regular basis.

Anti-bullying Policy

'3.2 We all have responsibility to respond promptly and effectively to issues of bullying/harassment.'
'Is secretive about their use of the internet, mobile phones and other technologies they have access to use'

'Does not show or choose to share what they are doing on the internet, mobile phones and other technologies they have access to use'

Behaviour for Learning Policy

The Academy Council's Policy on Rights and Responsibilities The Academy has the right:

- To expect students, parents/carers to adhere to the e-safety guidelines and the Acceptable Use Policy that they have signed.

The Academy recognises its responsibility:

- That any online learning space complies with e-safety guidelines and the Acceptable Use Policy, taking effective disciplinary action for any misconduct.

The Academy expects students:

- To work within the agreed e-safety guidelines and comply with the Acceptable Use Policy that they have signed.

The Academy expects parents/carers:

- To adhere to the Acceptable Use Policy and ensure that the students within their care work within the E-Safety guidelines

5 Disciplinary Sanctions (Disciplinary Penalties)

5.1 Specific Sanctions (Disciplinary Penalties) The Academy Council has agreed that the following 'disciplinary penalties may be used within the Academy:

Remove access to any online Oasis systems and Microsoft Office 365, the internet and any Oasis owned ICT equipment as appropriate to the incident – the Acceptable Use Policy provides guidelines for how individual Academies can set their own level of privileges.

Curriculum Policy (Primary)

Objectives

To realise our aims our curriculum must:

- Provide students with the ability to use a wide range of technological tools to further their independent learning strategies

Additionally, our curriculum must pay attention to the most significant needs of our local community.

These needs may include:

- Proficient use of a range of technological tools, together with awareness of maintaining personal safety and adopting responsible attitude towards the use of technology systems within their everyday life

Organisation and Strategies

- Learning resources will be made available for anytime learning through a robust virtual learning space that will enable all students to engage interactively. The resources and supporting documents will be mapped against the planned curriculum.

Outcomes

Oasis Community Learning will maintain a shared online learning space, enabling all staff, teachers, students and parents/carers to jointly celebrate, share and learn from one another. The tools provided within the online learning space give a secure way to introduce 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 Academy environment.

Teaching and Learning Policy & Guidance (Primary)

Objectives

Each student will be encouraged to:

- Learn to acquire information from a variety of sources and to record their findings in various ways according to their own preference, which will include a range of technological tools
- Develop knowledge, understanding and control of a wide range of technological tools to further their independent learning strategies
- Know how to work within e-safety guidelines within their everyday life

Expectations

- Allow students to choose their own ways of working to develop as independent learners that will include the selection of the appropriate technological tools
- Students will be able to study from any location; access to the Oasis Virtual Learning Platform will provide a series of technology learning tools and resources to help students to plan, collaborate, and receive feedback from teachers or other expert sources, including the use of video conferencing between sites, relating to their chosen subjects.

Classroom teachers will be expected to:

- Use a range of technological tools selectively and appropriately to enhance the teaching process and motivate students towards positive attitudes to learning, enabling them to take more responsibility for their own learning.
- Make effective use of the online Oasis systems and Microsoft Office 365 to develop effective engagement in learning from any location, including home and during educational visits.
- Provide situations to evaluate how well students understand how to work safely online both within the Academy and their everyday life and monitor students working online to ensure that they are working with e-safety guidelines
- Make sure that any incidents, either misuse of systems or access to undesirable internet websites is reported according to the E-Safety Policy *Support staff will be expected to:*
- Monitor students working online to ensure that they are working with e-safety guidelines *Students will be expected to:*
- Develop safe ways of working within the e-safety guidelines from the AOTP when making use of technological tools both in the Academy and when accessing resources remotely *Parents and carers will be expected to:*
- Ensure that they have an understanding of how their child can work safely online by following the Oasis E-Safety guidelines and complying with the Acceptable Use Policy.

Learning environment:

We believe that:

- Stimulating resources through any online Oasis system and Microsoft Office 365 should be available in a format appropriate to the students and accessible from a range of devices within the learning environment.
- The provision of secure storage areas for student's personal devices when not required will provide a solution so devices are not left unattended.

Parental/carers' Code of Conduct Policy

The Scope and Application of this Policy

- The policy aims to ensure that the following behaviours demonstrated by parents will be dealt with by the Academy:
- Misuse of systems, for example the online Oasis systems and Microsoft Office 365, or equipment provided by Oasis *Information for parents*
- Parents/carers will be expected to comply with the E-Safety Policy and Acceptable Use of Technologies Policy with any Home Agreement that Oasis issues regarding their child's use of the online Oasis systems and Microsoft Office 365 and Academy owned equipment.

Offsite activities and educational visits Policy

E-safety procedures

Personal devices

Oasis E-Safety and an Acceptable Use of Technologies Policies apply wherever Oasis systems or equipment may be used. Therefore, students should be reminded that they have signed an Acceptable Use Agreement for use of Oasis systems and equipment and this will apply to any activities or visits carried out as oasis students.

Mobile Phones

At the discretion of the Trip Leader, students are allowed to take mobile phones on educational visits but they should be used for emergency purposes only. However, as in Oasis, students will be responsible for their own belongings. For personal safety reasons, students should be advised not to carry any technological devices, for example mobile phones, iPads in a prominent and vulnerable position. On trips abroad, the cost implications of making calls from abroad should also be pointed out to students.

Mobile phones, however, can be a vital lifeline on exchange visits. Staff should make arrangements whereby they can be contacted at all times when the group is not under close supervision. Each student should have the contact telephone number and should know an emergency code, e.g. a word or a phrase, to be used to indicate that there is a serious problem and help is needed.

Appendix 13 - Guidance - Biometrics Information for Parents

13.1 Frequently asked questions

- Do you record images of fingerprints?

No. It is our policy never to store images of fingerprints anywhere on the system. Only mathematical representations of certain points of interest are recorded, typically between ten and forty depending on the characteristics of the finger. This information is encrypted and is called a template. This data is extremely secure in its encrypted form but even if it were not encrypted it is impossible to recreate the original image of the finger from this data. By scanning an image of your child's fingerprint, we can turn this information into a unique number. This unique number will then be used to replace their current swipe card.

- Can fingerprints be used by the police or a court of law?

No, we do not store an image of their fingerprint. The recorded templates are comprised of a set of numbers which represent each person. This set of numbers will be unique within populations of hundreds, or a few thousand, people. However, in the wider population the system is not accurate enough for the templates to be usable for forensic matching with any degree of certainty. A court of law would never be able to use this information as evidence.

- What happens when my child leaves the Academy?

As part of the Oasis Policy all data will be removed from the system once the student has left the Academy.

- How secure is the stored data?

Students, parents and staff can rest assured that the fingerprint images cannot be used by any other source for identification purposes. The system uses an image of the fingerprint to create a unique number and then discards the fingerprint from the system; only the numbers remain and these cannot be reinterpreted back into a fingerprint image.

- What would happen if somebody stole the data in some form?

The database is protected by a license key, which means that the database and any backup of its contents can only be accessed on licensed hardware. The licensed hardware is stored in the Academy's own secure facility, so that the encrypted data is only available to the registered licensee. Even if an Academy's security were to be compromised and a backup of the database stolen, the encrypted data would still be unreadable, even by another.

- If I object to my child's finger biometrics being taken, what will happen?

The Academy will issue any student who wishes to opt out of the biometric system with an alternative method of identification. Biometric system works with a number of identification methods, including smartcards, PIN numbers, passwords and name and photo lookup.

- Accessibility- Will there be any alternative for students who are unable to provide biometric data for some reason?

Alternative identification methods, such as name and photo look-up, where required will be made available in Biometric systems. Students unable to provide biometric data can opt to use one of these methods, as can any student who prefers not to use biometrics.

13.2 Cashless catering system information

A cashless system allows for parents (online) or students (using cash loaders) to top up a catering account before entering the canteen. This allows for quicker serving times and shorter queues. The system recognises each individual pupil, holds their individual account balances, and records money spent and received. It records where money is spent, on what food, and on any specific date, at any time of day.

- How are pupils recognised by the system?

Each pupil will create a finger biometric. A scan of the finger is taken and a template created (a string of encrypted numbers based off the finger scan). The rest of the finger image is discarded which makes reverse engineering the fingerprint from the data stored impossible. Pupils will then be able to use their finger biometric to identify on the system and authenticate actions.

- How is a finger biometric used to obtain a school meal?

The Pupil simply places their finger on the Biometric reader at the point of sale. A display will show the server the pupil's name and current account balance held within the system. The selected food items will be entered into the system from an itemised keyboard, while the amount spent and the new account balance will show on the display.

- How is money entered into the system?

(a) Online Payments (if available) allow a parent / Guardian to 'log-on' to a web portal using a secure username & password, and 'top-up' their child's account using debit and credit card payments.

(b) Coins and notes can be used to top-up accounts using Cash Loaders located at schools. They will accept £20, £10, and £5 notes, plus £2, £1, 50p, 20p, 10p and 5p coins. 1p and 2p coins, cannot be used.

(c) Cheque can be accepted too. Parents just need to send or hand in a check to the school with a payment made out to XXXXXXXX. A cheque box to receive payments will be located in the school. A payment covering any given period can be made via cheque i.e. a Term - 1/2 Term - Month - Week - Or a fixed monetary amount of your own choice.

- How does a pupil check what their current balance is?

daily spend limit of (£?????) (or a selected amount) will be set for all pupils and no food above that limit can be bought. On request, an individual pupil limit of your choice can also be set, to include a school dinner and break time snacks

- What about pupils entitled to a 'free school meal'?

The system works exactly the same for all pupils whether they pay or have a free school meal. All pupils have their own account and use it in exactly the same way regardless if on free school meals or not. The amount allocated for free school meals will simply be entered into the system by the software daily.

The system will then allow the required cash amount for each individual pupil to be allotted to their current account balance. However, any under spend or missed dinner will be identified by the system and will not be added to the next day's balance.

The parents or pupil can also add extra funds on to his or her account by using an on-site cash loader, or the online web-portal. This enables a greater daily spend on school dinners than allocated by their free meal allowance. As the free school meal allowance can only be spent on a school dinner, extra funds added into the system can be used for break time snacks. There will be no more queuing to be issued a 'free meal' tickets, or pupils' names entered into the 'free meal' register at the till point.

13.3 Biometrics Parent/Carer Opt-in Form

13.3.1 Parent/Carer information Letter

Dear Parent or Guardian,

I am excited to inform you that we will be implementing a new student recognition system using biometrics. This will allow us to make the best use of efficient solutions such as cashless catering, library management, print and copy cost control, access control, and registration.

We expect this system to improve the services we can offer students and staff significantly, with benefits including:

- Improved security for handling cash transactions in the school
- Reduction in administration time and cost dealing with lost or forgotten cards/passwords/PINs
- Reduction in opportunities for bullying (there is nothing that can be stolen for use by another student)
- Children will not have to remember to bring a card
- Reduction in queuing time

This is a technology that is already used successfully by thousands of schools and as a leadership team, we are convinced that this is the right way forward. We are keen to provide an opportunity for parents and guardians to find out more about the system and answer any questions they may have.

We would like to make it clear that [Oasis Academy XXXX] will comply at all times with Data Protection Regulations and with the provisions of the Protection of Freedoms Act 2012 (which came into force in September 2013) regarding the use of biometric data. For your child to use the biometric system, one parent or carer will need to read, consent by email, or sign and return the attached form. We will also offer an opportunity to opt out for those pupils who, upon consideration, would prefer to use alternative forms of identification.

If you would like more information or the chance to discuss this further, please feel free to contact me.

Yours faithfully,

[Insert name of Principal]

13.3.2 Parent/Carer Opt-in Biometric Consent Form

Should you agree to the processing of your child's biometric information, it is important that you return the signed consent form below as soon as possible. Please note that when he/she leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be permanently deleted from the live system.

If you would like to discuss this in more detail, please contact the school.

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Please complete this form if you consent to your child using biometric systems until he/she leaves the school.

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely and permanently deleted from the live system by the Academy.



I give consent to the school for the biometrics of my child: [insert name of child] to be used by Oasis Academy XXXXX for use as part of a recognition system as described above.

I understand that I can withdraw this consent at any time in writing.

Name of Parent:

Signature:

Date:



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