# E-SAFETY POLICY

**JULY 2018**

CONTENTS

Purpose ..... 4 a.

Policy Scope ..... 4

b. Policy Principles ..... 4

c. Policy Objectives ..... 4

d. Policy Strategy ..... 5

Definitions

..... 6

Related Oasis Policies, Standards and Processes ..... 7

Applicable Legislation, Guidance and References ..... 8

Applicable legislation ..... 8

References: ..... 9

Guidance ..... 10

Policy Statements ..... 11

1. Oasis Safeguarding Statement of Intent ..... 11

2. Academy Operational E-Safety Manual ..... 11

3. Roles and Responsibilities ..... 12

4. Acceptable User Agreements and Consent Forms ..... 12

5. Student use of Microsoft Office 365 Apps ..... 13

6. Student use of Personally Owned Devices ..... 13

7. Monitoring ..... 14

8. Unacceptable Use of Technology ..... 15

9. Student Accounts and Passwords ..... 16

10. Internet Access ..... 17

11. Email ..... 17

12. Publication ..... 18

13. Video Conferencing, Chat and Instant Messaging ..... 18

14. Social Media/Networking and Blogs ..... 19

15. Newsgroups, Forums and Personal Websites ..... 19

Appendix 1 - RACI Matrix ..... 21

Appendix 2 - Operational E-Safety Manual Template ..... 23

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

## Purpose

This E-Safety Policy applies without exception to all users of ICT facilities and equipment within Oasis Community Learning (OCL). This includes staff, students and any visitors who have been provided with temporary access privileges.

The purpose of this policy is to provide details of personal responsibilities and accountability for use of Oasis IT systems and devices.

The policy also contains guidance on the use of network resources which includes the use any online Oasis system, Microsoft Office 365, the internet, e-mail, instant messaging, social media, media publications, file transmission and voice communications.

This policy will be amended on a regular basis to take into account changes in best practice, legislation and wider Oasis Policy, so please check the policy portal for the latest version regularly.

a. Policy Scope

The 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. laptop computers at home; remote access to any online Oasis system and Microsoft Office 365 and networked resources.

The policy also covers the use of personally owned devices both on and outside of Oasis premises.

The contents of this document are fully compliant with the DfE statutory guidelines enforced from 03.09.2018 in 'Keeping Children Safe in Education (KCSiE)'. The legal requirements of the KCSiE guidelines are consistent with those designated as mandatory sections of an academy Operational ESafety Document. The Appendices within this document and the E-Safety policy statements cover the use of Oasis IT Services if applied correctly within Academies.

Oasis also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. This policy is designed to help Oasis academies to be compliant with this statutory duty.

b. Policy Principles

To use IT facilities at 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.

Parents/Carers are issued with a copy of the 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.

It is expected that all users will adhere to group password policy and guidelines in addition to all relevant regulatory and legal requirements. Details of the Password protocols are available in this document.

c. Policy Objectives

The objectives of this policy are to:

- Define every user's responsibilities when using Oasis IT systems.

- Define how regulations apply to users.
- Define consequences for misuse.
- Define who regulates the responsibilities, procedures that need to be in place to safeguard all users.

d. Policy Strategy

It is Oasis' policy to protect users from harm, so far as is reasonably practicable, whilst maximising the educational and social benefits of using technology. Oasis IT Services will ensure that all users of technology can be safe online when they are in the care of Oasis and will educate them to protect themselves when they are not in Oasis care. Consequently, when they use technology that is new to them, they will act in a responsible and safe way.

The policy has been developed to allow Oasis 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. The policy has been developed in the context of the Oasis Ethos and Nine Habits of behaviour.

Access to the internet is available for authorised users only and is provided to support work related activities and for educational purposes only.

To ensure compliance with the Oasis E-Safety, Oasis Acceptable Use of Technologies and the Oasis Use of Personally Owned Devices Policies, each Academy is responsible for setting in place an Operational E-Safety Manual.

All access to the internet at Oasis must comply with the Oasis Community Learning Web Filtering Policy and the Oasis Community Learning Web Filtering Change Process

Oasis operates an organisation-wide email system; where appropriate, staff and students will be provided with a unique Oasis account for their individual use.

All users will be deemed to be familiar with and bound by this E-Safety Policy. A copy of this policy can be found on the Oasis Community Learning Policy Portal.

Oasis IT Services maintain the right to access the unique Oasis account 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. This includes access to Home folders and email accounts.

Oasis IT Services recognise 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.

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

Video and photographic technologies are very powerful learning tools. However, any Oasis photographs and/or video may be taken by staff to support educational aims only.

## Definitions

**OCMS:** The Oasis Call Management System, used by Oasis IT Services and by system users to record incidents, requests, changes and problems within the operation of the IT System to be resolved.

Calls or tickets recorded in this system provide the identifier and audit trail of actions carried out by the Oasis IT Services team on the Oasis IT System and form the basis for recording authorisation for these works to be undertaken.

**Users:** Users are individuals who make use of the Oasis IT Services IT System. They include students, staff, contractors, consultants, temporary employees, volunteers, business partners, guests and visitors.

**User Account:** The most import component of a user's ability to gain access to an Oasis IT Services Managed Resource is the 'User account'. The user account is the basic identifier through which access is allowed or denied. User accounts are associated with a named person. The association may in the form of the account being assigned to an individual member of Oasis or it may be sponsored by an Oasis staff member who is accountable for its use but assigned to an individual who is not an Oasis employee or staff member.

**Web Filtering:** Is the restriction and prevention of access to individual and groups of websites based on the content. Oasis IT Services currently deploy a solution from the manufacturer Smoothwall to implement Web Filtering across the Oasis IT Services network.

## Related Oasis Policies, Standards and Processes

E-safety is of paramount importance, the E-Safety Policy states the Oasis stance on E-safety and how this should be implemented. E-safety References encourage frequent reviews of how effectively students are working within these guidelines. In addition, a series of resources and child protection tools will be available through the online Oasis systems and Microsoft Office 365.

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

- OCL Safeguarding
- 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 Data Protection Policy
- The Oasis Password Policy
- The Oasis Use of Personally Owned Devices (UPOD) Policy
- The Oasis IT Major Investigations
- The Oasis IT Access Policy
- The Oasis Information Security Policy
- The Oasis Web Filtering Policy
- The Oasis Data Retention Policy

- The Oasis IT Asset Management Policy
- The Oasis IT Device Monitoring Policy
- The Oasis IT Incident Management Policy
- The Oasis IT Change Management Policy
- The Oasis IT Request Fulfilment Policy
- The Oasis IT Problem Management Policy

## Applicable Legislation, Guidance and References

Applicable legislation

The user must comply with all the relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Copyright, Designs and Patents Act 1988 - www.legislation.gov.uk/ukpga/1988/48/contents
- Malicious Communications Act 1988 - www.legislation.gov.uk/ukpga/1988/27
- Computer Misuse Act 1990 - www.legislation.gov.uk/ukpga/1990/18
- Criminal Justice and Public Order Act 1994 - www.legislation.gov.uk/ukpga/1994/33/contents
- Trade Marks Act 1994 - www.legislation.gov.uk/ukpga/1994/26/contents
- Data Protection Act 2018 - www.gov.uk/data-protection
- Human Rights Act 1998 - www.legislation.gov.uk/ukpga/1998/42/contents
- Regulation of Investigatory Powers Act 2000 - www.legislation.gov.uk/ukpga/2000/23/section/1
- Freedom of Information Act 2000 - www.legislation.gov.uk/ukpga/2000/36
- Communications Act 2003 - www.legislation.gov.uk/ukpga/2003/21/contents
- Criminal Justice and Immigration Act 2008 - www.legislation.gov.uk/ukpga/2008/4/contents
- Keeping children safe in education - www.safeguardinginschools.co.uk/keeping-children-safein-education-2018/
- General Data Protection Regulation 2018 - www.eugdpr.org/eugdpr.org.html
- PREVENT - www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/preventstrategy-review.pdf

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

References:

Appendix 1 - RACI matrix

Identification of named personnel who are:

- Responsible
- Accountable
- Consulted
- Informed

Appendix 2 – Reference - Operational E-Safety Manual Template

- Academy-wide operational procedures
- Support for staff E-Safety procedures
- Mapping student experience of technologies in Oasis

Appendix 3 – Reference - Whole Academy Operational E-Safety, unacceptable use matrix and sanctions

- Matrix for acceptable and unacceptable use
- Sanctions matrix
- Decisions re use of communication technologies

Appendix 4 – Reference - Checklist Roles and Responsibilities

- Oasis Trust Group Executive
- Oasis National / Regional Directors / Data Protection Officer
- Oasis Academy Principals /ALT/DSL/ Data Protection Lead
- Oasis National / Regional / Site-based IT Support Teams
- Oasis Staff / External Agencies
- Oasis Students
- Parents / Carers

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)
- 5.2 Terms and Conditions - Acceptable Use of Technologies Agreement - Oasis Primary Key Stage 2 students
- 5.3 Terms and Conditions - Acceptable Use of Technologies Agreement – Oasis Secondary Students

  **NB** There are sample posters for Oasis Primary Key Stage 1 Students to use as part of their understanding before agreeing to their use of the Oasis IT systems in Appendix 7

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

- Sample of the route for escalating and reporting on E-Safety incidents.

Guidance

As further support, Guidance documents have been provided within the Appendices these should be used in conjunction with the References giving the position for Oasis Academies:

Appendix 7 – Guidance – Rules for students

Sample posters and information sheet to be used in conjunction with E-Safety sessions and displayed where there is use of IT systems, particularly for younger students who cannot read but still are required to agree before Oasis IT systems.

Appendix 8 - Guidance Use of technologies around Oasis Academy

Sample of a typical day where students have access to technologies throughout their journey from home to school and back again.

Appendix 9 – Guidance – Sample Home Use Agreement – Oasis Equipment

For potential editing for use when students are provided with Oasis IT equipment for personal use at home or off site.

Appendix 10 – Guidance - Developing safe use of Learning Technologies

Providing outline of the Oasis wide shared Microsoft Class Note Book that contains details of how the Office 365 tools can be used. Sections contained within the Note Book are:

- Learning, sharing and productivity tools
- Creativity tools
- Strategic development and tracking
- IT National Challenges
- Accreditation routes

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

Providing details of the 3 core Frameworks:

- Readiness for learning technologies;
- Identifying the Learning;
- Outstanding Digital Learners

Appendix 12 – E-Safety embedded into other 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

Appendix 13 - Biometrics information for Parents

## Policy Statements

1. Oasis Safeguarding Statement of Intent

1.1. Oasis Charitable Trust is wholly committed to ensuring that all children and adults at risk who engage with Oasis activities across the Oasis group through its subsidiaries (Oasis UK, Oasis Community Learning, Oasis College, Oasis Community Partnerships, Oasis Aquila Housing and STOP THE TRAFFIK), are cared for in a safe and secure environment. To fulfil this commitment, a number of safeguarding arrangements are in place.

1.2. We will ensure all policies and procedures in respect of safeguarding children are up to date and in line with Keeping Children Safe in Education 2018. The policies are accessible to all

staff through the Oasis Zone. Policies and procedures are reviewed and revised by the Oasis Board of Trustees on a regular basis.

1.3. As delegated by the Board of Trustees, the Oasis Group Chief Executive is the lead for Safeguarding Children and Adults at Risk and has oversight of the Oasis Group Policy Committee which reports to the Board on all Safeguarding issues.

1.4. Oasis is associated with the local Safeguarding Children Board of each Local Authority in which it operates. Any issues related to safeguarding children will be discussed at these boards as required.

1.5. Oasis meets statutory requirements in relation to Disclosure & Barring Service – all staff and volunteers who work with Oasis who meet the 'regulated activity test' (Freedoms Act 2012) is required to undergo an enhanced DBS check prior to employment.

1.6. The Board of Trustees for Oasis Charitable Trust has ultimate responsibility for Safeguarding issues. Operationally, this responsibility is delegated to the Group Chief Executive, who leads on policy issues in relation to the safeguarding of children and adults at risk across the Oasis Group. Within each subsidiary/operational area of activity across the Oasis Group there are Safeguarding Leads/Child Protection Officers who lead on Child Protection issues within their relevant location. They are clear about their role, have sufficient time and receive relevant support, and training, to undertake their roles, which includes close contact with outside agencies including social services, the Local Safeguarding Children's Board and relevant health care organisations.

1.7. All eligible staff and volunteers are required to undertake relevant safeguarding training and this is regularly reviewed by each lead in the Oasis subsidiaries to ensure it is up to date. A training database for all staff and volunteers is maintained, while training needs are reviewed as part of individual performance reviews and more broadly throughout the organisation by audit.

1.8. Oasis has robust audit checklists to ensure that safeguarding systems and processes are working. The audit includes: the monitoring of Academies Single Central Record, the monitoring of Child Protection & Adults at Risk Policies and Procedures including, 'Allegations against Professionals' and the monitoring of training for all employees and volunteers, guidance and support. The Oasis audit will be undertaken in December for reporting in January. When necessary, Oasis will take part in relevant audits with partner agencies including those from relevant Local Authorities.

## 2. Academy Operational E-Safety Manual

2.1. Every Oasis Academy is required to produce an Operational E-Safety Manual which is based on the content of this overarching E-Safety Policy.

2.2. The Operational E-Safety Manual must be able to demonstrate a robust and secure system and define how any incidents or infringements of an Academy's Operational E-Safety Manual are reported and dealt with according to their chosen Discipline and Sanctions policies.

2.3. The main considerations within the policy must be the safety of the individual users and the system itself.

2.4. To establish an operational document, the Operational E-Safety Manual Template in Appendix 2 should be used within an Academy's operational solution for E-Safety.

2.5. To support the decisions made when creating the Academy Operational E-Safety Manual, each Academy is required to undertake a risk analysis for the use of IT systems within the Academy and maintain an up to date E-Safety Risk Register.

2.6. When using the References outlined in the previous table, each Academy must explain the E-Safety procedures as will work within the Academy. The Policy should enable an Academy to be able to demonstrate and provide a clear explanation with evidence of:

- How any breaches of the E-Safety Policy will be documented, reported and dealt with.
  - How E-Safety training will be implemented for different users.
- How the Acceptable Use of Technologies Agreements will be explained, issued and signed by the different users of the Oasis system and equipment.
- Whole Academy planning and procedures.

2.7. When creating the Academy Operational E-Safety Document all the Reference areas in Appendix 2, 3 & 4 must be explicitly evidenced.

3. Roles and Responsibilities

3.1. Appendix 4 outlines the roles and responsibilities for the E-Safety Policy implementation within Oasis. An Academy is required to be able to demonstrate that they have defined the roles, responsibilities and accountability as outlined within their Academy Operational E-Safety Document.

3.2. In a small Academy, some of the roles described may be combined, though an Academy will need to ensure that there is sufficient "separation of responsibility" if this is the case. Whilst each individual is responsible for their own E-Safety, a detailed description for the role and responsibility for each of the following groups is defined with full descriptions in Appendix 4 .

3.3. Oasis has a responsibility to ensure that all reasonable and appropriate steps have been taken to protect users whilst using Information Technologies.

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

3.5. Oasis Academies 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 learning spaces as well as providing information about national and local E-Safety campaigns, for example Safe Internet Days: https://www.childnet.com/resources/safer-internet-day

4. Acceptable User Agreements and Consent Forms

4.1. Acceptable User Agreements form the agreement between any authorised user of Oasis IT systems and Oasis about Acceptable Use of these Oasis IT System.

4.2. Oasis have a standard Acceptable Use of Technologies Policy which applies to all users of the system.

4.3. A summary Acceptable Use Agreements must be issued to parents/carers which is available in Appendix 5

4.4. Parents will be expected to explicitly 'Opt-out' if they do not want their child to make use of the OCL IT systems, internet or email.

4.5. Appendix 5 contains Terms and Conditions of the agreements that a user will accept and agree to comply with by clicking on the online 'Agree' disclaimer. The Terms and Conditions for their agreement are also available from a link on the Disclaimer page.

4.6. Individual users will be required to agree to this Oasis E-Safety Policy when they log-in to the Oasis IT System or devices. When accessing the system for the first time they will have to agree to the following online statement prior to gaining access to the Oasis IT systems:

"By clicking on the "I Agree" button below and logging into the Oasis Community Learning domain, you agree to abide by the terms of Oasis Community Learning Acceptable User Agreement, the Oasis E-Safety and the Use of Personally Owned Devices Policies.

The type of material you access on the Internet is strictly monitored and filtered.

You are responsible for making sure that you act in accordance with all IT policies, other named policies and legislation applicable to the Oasis Community Learning network.

**If you do not agree to these please do not use the OCL IT Systems"** I Agree

4.7. There are age appropriate Acceptable Use of Technologies Agreements available for different age groups and/or role(s) within an Academy. A sample resource for Reception and Key Stage 1 students to be given and discussed prior to them clicking on the on-screen 'Agree button'. A Guidance sample of this is provided in Appendix 7.

4.8. Academies may add further clauses into these documents before they are used but these are the level expected of all users. Academies should provide a clearly defined use of statements that match the Academy version of any Reference Documents (in conjunction with these Agreements) with planned review and monitoring sessions scheduled throughout the academic year.

4.9. The use of Biometric information required separate explicit opt in permission. Appendix 13 contains information about how and why biometric information is gathered, stored and used within Oasis Community Learning Academies and some sample forms etc. that can be used to support the gathering of this consent.

5. Student use of Microsoft Office 365 Apps

5.1. Microsoft Office 365 is part of the core platform provided by Oasis IT Services and used in Oasis to support both the administrative and teaching and learning aspects of the organisation.

5.2. At its core Microsoft Office 365, is a web-based platform that facilitates sharing and collaboration between users. This both presents huge opportunities in terms of teaching and learning and productivity as well as presenting some significant E-Safety Risks which need to be managed at each Oasis Academy.

5.3. As part of the drive to ensure effective and safe use of the Microsoft Office 365 each Academy needs to determine the level of use they expect for authorised users and in particular students. Academy will need to make special request for students in Year 3 and below to have access to the Internet and Office 365 Apps as referred to in Section 9.

6. Student use of Personally Owned Devices

6.1. Oasis Community Learning recognises the importance of technology and the educational benefits available using technology. The use of portable electronic devices in the classroom can add educational value when such devices deliver content and extend, enhance or reinforce the student learning process. Classroom teachers determine the appropriateness of in-class use of electronic devices, consistent with strategic objectives, and with approval of the Academy Principal.

6.2. All personally owned electronic devices must be used in a responsible, and legal manner. Students using their personally owned devices are subject to the Oasis Acceptable Use of

Technologies, E-Safety, Use of Personally Owned Devices (UPOD) Policies and all other Oasis policies and procedures, including but not limited to the student code of conduct. Failure to adhere to these guidelines may result in the revocation of the privilege to use personally owned devices in the classroom and/or disciplinary action as appropriate.

6.3. Student Mobile Phone and Personal Electronic Communication Device use is not permitted in any Oasis Academy. Oasis Community Learning operates a zero-tolerance policy of "see it, hear, it, lose it."

6.4. Mobile Phone and Mobile Personal Electronic Communication Device use is permitted as part of designed curriculum and must be explicitly approved by a Regional Director following discussion with the Academy Principal.

6.5. Where the use of Mobile Phones or other Personal Electronic Communication Device is being considered as part of the curriculum, Academy Principals should consider the disadvantaged communities that we serve and that not all children will have access to a personally owned device. Therefore, due consideration must be given to equality of access to the curriculum for all children.

6.6. Where use of Mobile Phones and/or Mobile Personal Electronic Communication Device is approved, the Academy Principal is accountable for ensuring that clear risk assessments have been undertaken and appropriate operating procedures are in place. A decision about student access to the internet from personally owned devices should be explicitly stated within the Academy Operational E-Safety Document.

6.7. Where Mobile Phones are approved for use, a sign must be displayed on classroom doors when the teacher is allowing their use.

6.8. To make sure that there is a clear transition into the learning environment where students and staff may make use of their personally owned devices and can make full use of OCL resources within the Microsoft Office 365 environment, the key Policy Statements from the Oasis Use of Personally Owned Devices (UPOD) should be incorporated into the Academy Operational ESafety Document and implemented accordingly.

## 7. Monitoring

7.1. Oasis IT Services reserve the right to monitor email, telephone and any other electronicallymediated 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

7.2. All users of Oasis ICT facilities or equipment expressly waiver any right of privacy and therefore should have no expectations of privacy in anything they create, store, send or receive using Oasis' ICT systems and equipment.

7.3. Oasis staff who have access to personal data, including data generated as part of system monitoring, (as defined under the Oasis Data Protection Policy) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

7.4. Oasis Community Learning makes use of a monitoring solution 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.
Academy DSLs are responsible for administering and monitoring this system. 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.

8. Unacceptable Use of Technology

8.1. Unacceptable use of computers, mobile devices (including phones) and network resources can be summarised as:

- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
- Threatening, intimidating or harassing employees and students including any message that could constitute bullying or harassment, e.g. on the grounds of sex, race, disability, religion or belief, sexual orientation or age.
- Using obscene, profane or abusive language.
- Using language that could be calculated to incite hated against any ethnic, religious or other minority group.
- Using or distributing any materials that are indecent which includes:
    - a child (under 18) sharing an indecent image (including images of themselves) with a peer (also under 18);
    - a child (under 18) sharing an indecent image (including images of themselves) with an adult;
    - a child (under 18) sharing an indecent image created by another child with a peer or an adult;
    - a child (under 18) in possession of a sexual image created by a child (under 18).
    - An Adult in possession of a sexual image created by a child (under 18).
    - An Adult sharing an indecent image (including images of themselves).

  Examples of indecent images include but are not limited to:
    - naked pictures; ○ topless pictures of a girl; ○ pictures of genitals;
    - sex acts including masturbation; and ○ sexual pictures in underwear.

- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.
- Defamation (genuine scholarly criticism is permitted).
- Unsolicited advertising often referred to as “spamming”.
- Sending emails that purport to come from an individual other than the person sending the message using, e.g. a forged address.
- Attempts to break into or damage computer systems or data held thereon.
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software.
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised.
- Using the network for unauthenticated access.
- Using the ICT facilities to conduct personal commercial business or trading.

Restrictions should be taken to mean, for example, that the following activities will normally be a breach of policy:

- Downloading, distribution, or storage of music, video, film or other material, for which you do not hold a valid licence or other valid permission form the copyright holder.
- Distribution or storage by any means of pirated software.
- Connecting an unauthorised device to the network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use.

- Circumvention of network access control.
- Monitoring or interception of network traffic, without permission.
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission.
- Associating any device to network Access Points, including wireless, to which you are not authorised.
- Non-academic/non-business-related activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs.
- Excessive use of resources such as file storage, leading to a denial of service to others, especially when compounded by not responding to requests for action.
- Frivolous use of ICT suites, especially where such activities interfere with others' legitimate use of ICT services.
- Use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.
- Copying of other peoples' website material without the express permission of the copyright holder.
- Use of peer-to-peer and related applications. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA.

8.2. Staff and students should consider the spirit of the Oasis Ethos when working on Oasis ICT systems. Any conduct which may discredit or harm Oasis, its staff or the ICT facilities or can otherwise be considered intentionally unethical is deemed unacceptable.

8.3. Incidents of misuse will be dealt with by Oasis in accordance with the Behaviour for Learning Policy (students) or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff). The appropriate level of sanctions will be applied as determined by the nature of the reported misuse. A matrix for student-related incidents which could occur and need consideration within an Academy can be found in the Appendix 2 Operational E-safety Manual Template.

8.4. 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 within the Academy Operational E-Safety Document. Consideration should be given to the Appendix 2 - 3.4.6 Mobile phones/portable devices for what an Academy decides is acceptable or unacceptable use within the Academy.

9. Student Accounts and Passwords

9.1. Each student will have their own, individual OasisNet account which is used to access Oasis IT Systems. Access will be granted as per the Oasis IT Access Policy.

9.2. Password Policy will be implemented as per the Oasis Password Policy.

9.3. The use of shared accounts or class accounts is not permitted for students who are in year one or higher. User accounts are issued by Oasis IT Services for individual use only.

9.4. With the advent of increasingly sophisticated password cracking programs, steps have been taken to minimise the problem posed by malicious users trying to break into accounts. The security of passwords used for accounts held on Oasis' servers is a highly important issue. The passwords used should be carefully considered as badly chosen passwords have the potential to be cracked or easily guessed.

9.5. For staff and Students (Year 4 above) passwords must be at least 12 characters long and should be a combination of letters and numbers.

9.6. For a younger student (Reception – Year 3) a simpler password is allowed but must be at least 4 characters long. Younger students using the simpler password will not have access to Internet facing services including Microsoft Office 365 or email from their unique accounts. Should an Academy wish for students to have access to Internet facing services, Office 365 and email (or any one of these functions) they will have to agree to the Password Policy used with older students and other users.

9.7. A password must not be based on anything connected with the individual who owns the account. This includes anything associated with a name or initials, job description, address or postcode.

9.8. Any passwords generated for use by Oasis IT Services should be changed immediately after initial use.

9.9. Accounts and passwords must not be shared, given away or offered for use to anybody else.

9.10. 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.

9.11. Staff are not permitted to maintain lists of student passwords.

10. Internet Access

10.1. Oasis implement network level filtering 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.

10.2. The Oasis filtering software 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 the person responsible for ICT within Academy, providing details of the site, including the web address, to reduce the possibility of the material being accessed again in future. The person responsible for ICT will then 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.

10.3. Students should be taught to be critically aware of the materials they read on the internet and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

10.4. Unacceptable use of the internet is detailed in this E-Safety Policy. As a rule, users should remember that they are acting as a representative of Oasis Community Learning and should always have due regard for Oasis policies and legislation when using the internet.

11. Email

11.1. 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.

11.2. 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.

11.3. 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.

11.4. If an offensive email is received by any user, the Oasis IT Services Desk team or a person responsible for ICT within the Academy must be contacted immediately so that appropriate measures can be taken. Students who choose to misuse the email system will be subject to disciplinary procedures by Oasis.

11.5. Email sent to an external organisation from an Oasis account should be written carefully. Personal email or messaging during employment at Oasis should not take place and personal email between staff and students is forbidden. Abuse of the use of email may lead to disciplinary consequences for both staff and students.

11.6. 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.

## 12. Publication

12.1. Any named images of students will only be published with the separate, explicit written consent of their parents or carers. Publishing includes, but is not limited to:

- Oasis web sites
- Web broadcasting
- TV presentations
- Newspapers

12.2. Care must be taken when capturing photographs, videos or using video-conferencing to ensure that all students are appropriately dressed and explicit written permission for use has been gained from parents and carers in line with normal guidance. This may be altered or amended at any time by the parent or carer through explicit written request.

12.3. Student's work will only be published if the parent's or carer's explicit written consent is received. This may be altered or amended at any time by the parent or carer by explicit written request.

## 13. Video Conferencing, Chat and Instant Messaging

13.1. Students will be allowed to use video conferencing 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.

13.2. Oasis maintains a series of online communication/ messaging tools, including websites and through Microsoft Office 365 with Skype for Business. This enables staff, teachers, students and parents/carers to jointly celebrate, share and learn from one another. The tools provided within any online Oasis 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. These tools include blogs, forum and a video conferencing/IM solution.

13.3. Online conferencing is a powerful method for students and staff to share information and opinion. However, some conferencing applications, including chat and newsgroups sometimes attract undesirable and irrelevant comment. Open access to un-moderated newsgroups by contributors means that newsgroups can be infiltrated by the immature and offensive and for this reason, may not be made available in Academies.

13.4. Skype for business is made available for staff members by default but not for students. Academies may request access to Skype for Business for students in order to support curriculum activities following the production of a suitable risk assessment and with approval of a Regional Director.

13.5. Oasis IT Services are able to retrieve chat/instant message conversations undertaken using the Skype for Business Platform.

13.6. The use of other chat / instant messaging tools on the Oasis network is prohibited. Access to these tools will not be allowed by Oasis IT Services without a written instruction from the Chief Executive Officer.

14. Social Media/Networking and Blogs

14.1. As part of the curriculum E-Safety sessions where students will be instructed about access to social networking sites and how such websites will be used within an educational context; students will be told about the restrictions that apply to personal use and how they hold personal responsibility to protect their personal information.

14.2. Oasis realises that the majority of young people are using social networking sites at home. We aim to make students responsible users of these sites and therefore students should be made aware of the advantages and dangers of using these websites.

14.3. Oasis IT Services will filter Social Media to prevent its access to the network by default. However, as with all forms of Web filtering it is possible that access, inadvertent or otherwise may be possible to some services. Users, other than those who have specifically been granted to permission are prohibited from making use of Social media services from within the Oasis Network.

14.4. Users who may be specifically granted permission may include staff members and others who are responsible for the organisation's online and social media presence as part of their assigned duties.

14.5. Access to Social Media websites will only be granted as the Oasis Web Filtering Change Process.

14.6. It is relatively straight forward for an individual to create a personal blog. Blogs are often hosted within common blog hosting services. 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 is deemed to be inappropriate then the IT Service Desk should be notified immediately so that access can be restricted.

15. Newsgroups, Forums and Personal Websites

15.1. The internet provides access to a very large number of forums and Newsgroups which allow individuals to communicate and discuss particular topics. Many of these areas are unmoderated and the content can differ significant 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.

15.2. 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 curriculum E-Safety sessions 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.

15.3. The posting of information by students to public Newsgroups and Forums as part of the curriculum requires specific authorisation from a Regional Director.

15.4. 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.

15.5. 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.

15.6. The development of personal websites by students constitutes the publication of their work and therefore is subject the requirements of section 12 of this document.

15.7. 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 apposition to edit or remove content that has been published as part of the site without reference to the student.

## Appendix 1 - RACI Matrix

| Policy Element | | Leadership | | | | Academy | | | | | | Services | | IT Team | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Policy Owner | Group CEO | OCL CEO | OCL COO | Regional Director | Academy Principal | Designated Representative | Designated Data Protection Lead | Teacher | Academy User | Students | Head of National Service | National Service User | Director of IT Services | National Service Delivery Manager | National Infrastructure Manager | National Programme Manager | National IT Operations Manager | Data Protection Officer | Service Desk Manager | National Service Desk | Regional Service Delivery Manager | Cluster Manager | Onsite Teams |
| Policy: Purpose; Principles; Strategy; Legal Constraints; 1. Oasis Safeguarding Statement (National) | A | I | I | C | C | I | | I | | | | I | I | R | I | I | I | I | R | I | I | C | | |
| 2.1 ➔ 2.7 Academy Operational E-Safety Manual | | I | I | C | C | A | R | R | I | I | I | I | I | C | I | I | I | I | C | I | I | I | I | I |
| 3.1 ➔ 3.5 Roles and Responsibilities (Academy) | | | | | I | A | R | R | I | I | | I | I | C | I | I | I | I | C | I | I | I | I | I |
| 3.1 ➔ 3.5 Roles and Responsibilities (National) | | | I | I | A | R | I | I | | | | I | I | R | I | | | | C | I | | I | | |
| 4.1 ➔ 4.9 Acceptable Use Agreements (Academy) | | | | | I | A | R | R | I | I | I | I | I | C | I | I | I | I | C | I | I | I | I | I |
| 4.1 ➔ 4.9 Acceptable Use agreements (National) | | | I | I | A | R | I | I | | | | I | | R | I | | | | C | I | | I | | |
| 5.1 ➔ 5.3 Student use of Office 365 Apps (Academy) | | | | C | R | A | C | C | I | I | I | I | I | R | I | I | I | I | C | I | I | I | I | I |
| 5.1 ➔ 5.3 Student use of Office 365 Apps (National) | | | | A | I | R | I | I | | | | R | I | R | I | | | | C | I | | I | | |
| 6.1 ➔ 6.8 Student use of personally owned devices (Academy) | | | I | | I | A | R | R | I | I | I | | I | C | I | I | I | I | C | I | I | | I | I |
| 6.1 ➔ 6.8 Student use of personally owned devices (National) | | | | A | R | C | | I | | | | R | I | R | I | | | | C | I | | I | | |
| 7.1 ➔ 7.4 Summary of Monitoring (Academy) | | | | I | C | A | R | R | I | I | I | | | C | I | I | I | I | C | I | I | C | I | I |
| 7.1 ➔ 7.4 Summary of Monitoring (National) | | | | I | I | I | | C | | | | | | A | R | I | C | | I | I | I | R | I | |
| 8.1 ➔ 8.4 Unacceptable use of Technologies (Academy) | | | | I | I | A | R | R | I | I | I | | | C | I | I | I | I | I | I | I | R | I | I |
| 8.1 ➔ 8.4 Unacceptable use of Technologies (National) | | | | I | I | I | I | I | I | | | | | A | R | I | C | | I | I | I | R | I | |
| 9.1 ➔ 9.11 Student Accounts and Passwords (Academy) | | | | I | C | A | R | R | | | | | | C | I | I | I | I | I | I | | C | I | |
| 9. 1 ➔ 9.11 Student accounts and Passwords (National) | | | | I | R | A | | | | | | C | | R | I | | I | | C | | | I | | |
| 10.1 ➔ 10.4 Internet (Academy & National) | | | | I | I | C | I | | I | I | I | I | I | A | C | C | I | C/I | R | I | I | R | I | I |
| 11.1 ➔ 11.6 Email (Academy) | | | | I | C | A | R | R | I | I | I | C | | R | C | I | I | I | I | I | I | I | I | I |

| Policy Element | | Leadership | | | | Academy | | | | | | Services | | IT Team | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Policy Owner | Group CEO | OCL CEO | OCL COO | Regional Director | Academy Principal | Designated Representative | Designated Data Protection Lead | Teacher | Academy User | Students | Head of National Service | National Service User | Director of IT Services | National Service Delivery Manager | National Infrastructure Manager | National Programme Manager | National IT Operations Manager | Data Protection Officer | Service Desk Manager | National Service Desk | Regional Service Delivery Manager | Cluster Manager | Onsite Teams |
| 11.1 ➔ 11.6 Email (National) | | | | A | C | I | | I | | | | C | I | A | C | C | I | I | C | I | | R | | |
| 12.1 ➔ 12.3 Publication (Academy) | | | | I | C | A | I | I | I | I | I | I | I | A | I | R | I | I | I | I | I | R | I | I |
| 12.1 ➔ 12.3 Publication (National) | | | | I | C | C | I | I | I | I | I | I | I | A | I | R | I | I | R | I | I | R | I | I |
| 13.1 ➔ 13.6 Video conferencing, chat and instant messaging (Academy) | | | | I | C | C | I | I | I | I | I | I | I | A | I | R | I | I | I | I | I | R | I | I |
| 13.1 ➔ 13.6 Video conferencing, chat and instant messaging (National) | | | | I | C | A | R | R | I | I | I | I | | C | C | C | I | I | C | I | I | R | I | I |
| 14.1 ➔ 14.6 Social media/networking and Blogs (National) | | | | I | I | I | | | | | | C | I | A | I | C | I | | C | I | I | R | | |
| 14.1 ➔ 14.6 Social media/networking and Blogs (Academy) | | | | I | C | A | R | R | I | I | I | I | I | R | C | C | I | I | C | I | I | R | I | I |
| 15.1 ➔ 15.7 Newsgroups, Forums and Personal websites (National) | | | | I | I | I | | | | | | C | I | A | I | C | I | | C | I | I | R | | |
| 15.1 ➔ 15.7 Newsgroups, Forums and Personal websites (Academy) | | | | | | | | | | | | | | | | | | | | | | | | |
| Appendix 2 – Reference - Operational E-Safety Manual template | A | | | I | | | | | | | | | | R | | | | | | | | | | |
| Appendix 3 – Reference - Whole School Checklist, unacceptable use and sanctions | A | | | I | | | | | | | | | | R | | | | | | | | | | |
| Appendix 4 – Reference - Roles and Responsibilities | A | | | I | | | | | | | | | | R | | | | | | | | | | |
| Appendix 5 – Reference -Acceptable Use of Technology Agreements | A | | | C | | | | | | | | | | R | | | | | | | | | | |
| Appendix 6 – Reference – Flow Diagram E-Safety Incident Reporting | A | | | C | C | C | C | | | | | | | R | | | | | | | | | | |

## 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<br>• Academy strategy for use of Technologies | Academy statement of vision for use of technologies and embedded E-Safety programme<br>***Guidance:***<br>***E-Safety Policy***<br>Appendix 10<br>Developing safe use of learning technologies |
| • Procedures for use of Technologies around the Academy | ***Guidance:***<br>***E-Safety Policy***<br>Appendix 8<br>Use of technologies around Oasis Academies |
| • Acceptable use of Technologies Agreements:<br>○ Oasis Staff ○ Oasis Students | **Reference:**<br>***E-Safety Policy***<br>Appendix 5<br>Acceptable User Agreements ***Guidance:***<br>***E-Safety Policy***<br>Appendix 7<br>Resource for discussing Agreement with Reception, Key Stage 1 students |
| • Home Use Agreement – Oasis equipment | ***Guidance:***<br>***E-Safety Policy***<br>Appendix 9<br>Sample Home Use Agreement – Oasis Equipment |
| • Biometrics Parent/Carer information and Opt-in Form | **References:**<br>***E-Safety Policy***<br>Appendix 13 Biometrics Parent/Carer information<br>Parent/Carer Opt-in Form |
| • Use of Personally Owned Devices | **References:**<br>***E-Safety Policy***<br>Use Personally owned devices |
| 2 Whole Academy planning for E-Safety | **Reference:**<br>***E-Safety Policy***<br>Appendix 3<br>Checklist for whole Academy E-Safety procedures ***Guidance*:**<br>***E-Safety Policy***<br>Appendix 11 |

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

# 1 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 Aspinal, 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 eSafety 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
- 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 Aspinal, we to 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.

Staff:

- All staff are given the Academy e-safety Policy and its importance is explained

Parents:

- Parents' attention is drawn to the Academy e-safety Policy in newsletters and on the Academy 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 Aspinal, eSafety is taught through the curriculum (as part of the Computing curriculum). The eSafety 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 eSafety policy. Access to inappropriate websites is blocked.

*2.4.2 Email*

Pupils do not have access to emails in school

*2.4.3 Webmail*

Pupils do not have access to webmail in school

*2.4.4 Chat Rooms*

Pupils do not have access to chat rooms in school

*2.4.5 Instant Messaging*

Pupils do not have access to instant messaging in school

*2.4.6 Mobile phones/portable devices*

Pupils do not have access to mobile phones in school

*2.4.7 Camera phones*

Pupils do not have access to camera phones in school

*2.4.8 Webcams*

Pupils do not have access to webcams in school

*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.

# 3 Academy procedures for Incidents, escalation points and sanctions

## 3.1 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 | | | |

## 3.2 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 | | | | | | |
| Unauthorised use of non-educational sites during lessons or websites not relevant to current learning | x | | | | | | | | |
| Unauthorised use of any personal device | x | | | | | | | | |
| Unauthorised use of social networking / instant messaging / personal email / chat rooms | x | | | | | x | | | |
| Unauthorised downloading or uploading of files | | x | | | | | | | |
| Allowing others to access Oasis network by sharing user names and passwords | | | x | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Attempting to access or accessing Oasis network using another student's account | | | x | | | | | x | |
| Attempting to access or accessing Oasis network using the account of a member of staff | | | x | | | | | x | |
| Corrupting or destroying the data of other users | | | x | | | | | x | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | | x | | | | | x | |
| Continued infringement of the above following previous warnings and sanctions | | | 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 | | | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | 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 | x | | x |

## 3.3 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 |
| Use of personal email addresses in Academy or on Academy network | | | | | | | | 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 | | | | |

EXPLANATION RE PERMISSIONS FOR CONTENTIOUS USAGE (IF APPROPRIATE)

# 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

## 5 Academy Risk Register

*Oasis IT Services have provided a template Excel file for an Academy to create a Risk Register with related concerns and implications for the use of technologies within an Academy*

E-Safety Risk Register Template.xlsx

## 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? |
| Are a wide range of users consulted when policies are being reviewed, re-written? |
| Who is responsible within Oasis Academy for E-Safety operational procedures? |
| Are all users familiar with the Oasis E-Safety Policy and the Academy Operational E-Safety Document? |
| Are there clear rules and guides visible in areas where students access technologies? |
| Do all users know how to report incidents, such as inadvertent access to undesirable websites/images? |
| 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? |
| Do all users know what sanctions could be applied for misuse of Oasis IT systems and equipment? |
| Are Oasis E-Safety procedures and reports regularly reviewed within school? |

### 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? |
| Is training directed to their specific role in the Academy? |
| Is there a clear process for supporting staff in the E-Safety development? |
| Is there a clear process for staff to report any difficulties or concerns they may encounter? |
| Do staff receive training on information literacy skills? For example, how to search and evaluate validity of information effectively? |
| Do new staff have an introduction to the Oasis E-Safety Policy and the Academy Operational ESafety Document as part of their induction? |
| Are staff expected to incorporate E-Safety activities and awareness within their curriculum areas? |
| Are the E-Safety activities and awareness sessions monitored, co-ordinated and supported across the Academy? |

### 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

| |
|---|
| Are students given an opportunity to contribute to Academy E-Safety procedures? |
| 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? |
| Do you know about a student's prior exposure to technologies? |
| 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? |
| Does the Academy have a framework for teaching E-Safety skills? |
| Does the Academy provide appropriate opportunities within a range of curriculum areas to teach E-Safety? |
| How does the Academy go about educating students of their exposures to the dangers of technology outside of Academy? |
| How is students' understanding of E-Safety issues assessed or measured? |
| 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? |
| Are students aware of the impact of online bullying, from the perspective of both the victim and the tormentor? |
| Do they know how and where to seek help if they are affected by online bullying? |

**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? |
| Are there individual logins to all accessible websites and security time-outs? |
| Does the Academy use a safe list of websites? |
| Are students taught how to critically evaluate materials as well as learning good searching skills? |
| Are students taught the importance of intellectual property regarding materials they find on the internet? |
| Are students aware of the Academy's policy on downloading materials from the internet? |
| 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? |
| **Email** |

| |
|---|
| Do students have access to email in the Academy? Is this applied by the account permissions or Academy requested access? |
| 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? |

| |
|---|
| How is student email use monitored, and are students aware of this? |
| Are students aware of the Academy's policies on email attachments? |
| Do students know how to virus-check attachments, both incoming and outgoing? |
| Are students aware of the seriousness of bullying by email? |
| Is this incorporated in the Academy's anti-bullying policy? |
| Are all students aware that there are sanctions for misuse of email on the Oasis network? |
| **Webmail** |
| Do students know Oasis' policy on webmail services? |
| Do students know how to use webmail services safely outside the Academy, for example by looking for privacy statements when registering for webmail accounts? |
| Do students know how to use inbuilt junk mail filters within webmail services? |
| Are students aware of the issues surrounding spam and spoofing? |
| Are students taught appropriate strategies for recognising and dealing with spam? |
| Are instructions given within the Academy to help minimise spam? |
| **Chat Rooms** |
| Are students aware of the safety issues relating to using chat rooms? |
| Are students aware how to safely negotiate online relationships? |
| Are students aware of the importance of keeping personal information private when chatting? |
| Are students aware of the dangers of arranging offline meetings with people they have met online? |
| Is use of any chat room permitted within the Academy? If so, is this for classroom use only? |
| **Instant Messaging** |
| Is access to instant messaging services permitted within the Academy? For example, the classroom uses of Skype for Business. |
| Are students aware of the safety issues relating to instant messaging? |

| |
|---|
| Do students know how to protect personal information when registering for instant messaging services, and how to set up closed groups or buddy lists? |
| Do students know where to get help and advice if they experience problems such as unwanted messages or bullying by instant messaging? |
| **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) |
| 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? |
| What are the sanctions for misuse? |
| If personally owned mobile phones are not permitted within the Academy, how is the policy enforced? |
| 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? |
| 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? |
| 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? |
| **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? |
| 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? |
| **Peer-to-peer networks** |
| Is access to peer-to-peer services required for student use and therefore permitted within the Academy? |
| If not, are such services appropriately blocked on the Academy's network? |
| Are students aware of the safety issues relating to peer-to-peer networks? |
| 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? |

| |
|---|
| Are students aware of their responsibilities with regards to illegally downloading or uploading materials to peer-to-peer networks? |
| **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 |
| Are systems in place to ensure the ethical use of data collected? |
| Are systems in place to ensure the validity of the information contained within the third-party site? |
| Does the Academy have/require a 'gatekeeper' for third-party sites such as the role of Data Protection Lead? |

**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 | | | | | |
| On-line gaming (non-educational) - Academy decision | | | | | |
| On-line shopping/commerce - Academy decision | | | | | |
| File sharing - Academy decision | | | | | |
| Use of social network sites - Academy decision | | | | | |
| Use of video broadcast sites, e.g. YouTube, Vimeo - Academy decision | | | | | |

**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 | | | | | | | | | |
| Unauthorised use of non-educational sites during lessons or websites not relevant to current learning | | | | | | | | | |
| Unauthorised use of any personal device | | | | | | | | | |
| Unauthorised use of social networking / instant messaging / personal email / chat rooms | | | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | | | |
| Allowing others to access Oasis network by sharing user names and passwords | | | | | | | | | |
| Attempting to access or accessing Oasis network using another student's account | | | | | | | | | |
| Attempting to access or accessing Oasis network using the account of a member of staff | | | | | | | | | |
| Corrupting or destroying the data of other users | | | | | | | | | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | | | | | | | | |

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

**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 | | | | | | | | |
| Academy policy supports the use of mobile phones in lessons | | | | | | | | |
| Academy policy supports the use of mobile phones in social time | | | | | | | | |
| Taking photos on devices with inbuilt cameras | | | | | | | | |
| Use of personal email addresses in Academy or on Academy network | | | | | | | | |
| Use of chat rooms / facilities | | | | | | | | |

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

## 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 | |
| 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 | |

### 2 Regional Directors

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

### 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 | |
| Are responsible for updating and maintaining an effective Academy Operational ESafety 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. | |

## 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. | |
| 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 | |

## 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. | |
| 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 | |

| | |
|---|---|
| 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 | |

## 6 Oasis students

| Aspect | Check |
|---|---|
| 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. | |

## 7 Parents/Carers

| 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 | |
| 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:**

- × share my username, password or personal information with anyone else
- × 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
- × deliberately misuse or deface another users' work on the Oasis network.
- × access or try to access any illegal material;
- × download files without permission;
- × get around or try to get around the Oasis network security measures
- × use or amend images or text that may cause distress or offence;
- × bring material into Oasis that has not been virus checked;
- × 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;
- × 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;
- × 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;
- × use another person's account at any time;
- × intentionally misuse Oasis blogs, Oasis Instant Messaging (Skype for Business) or Oasis accounts;
- × access or try to access chat rooms, forums, messaging, social networking or sites with gambling or adult content;
- × use IT equipment for fraudulent purposes;
- × 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:**

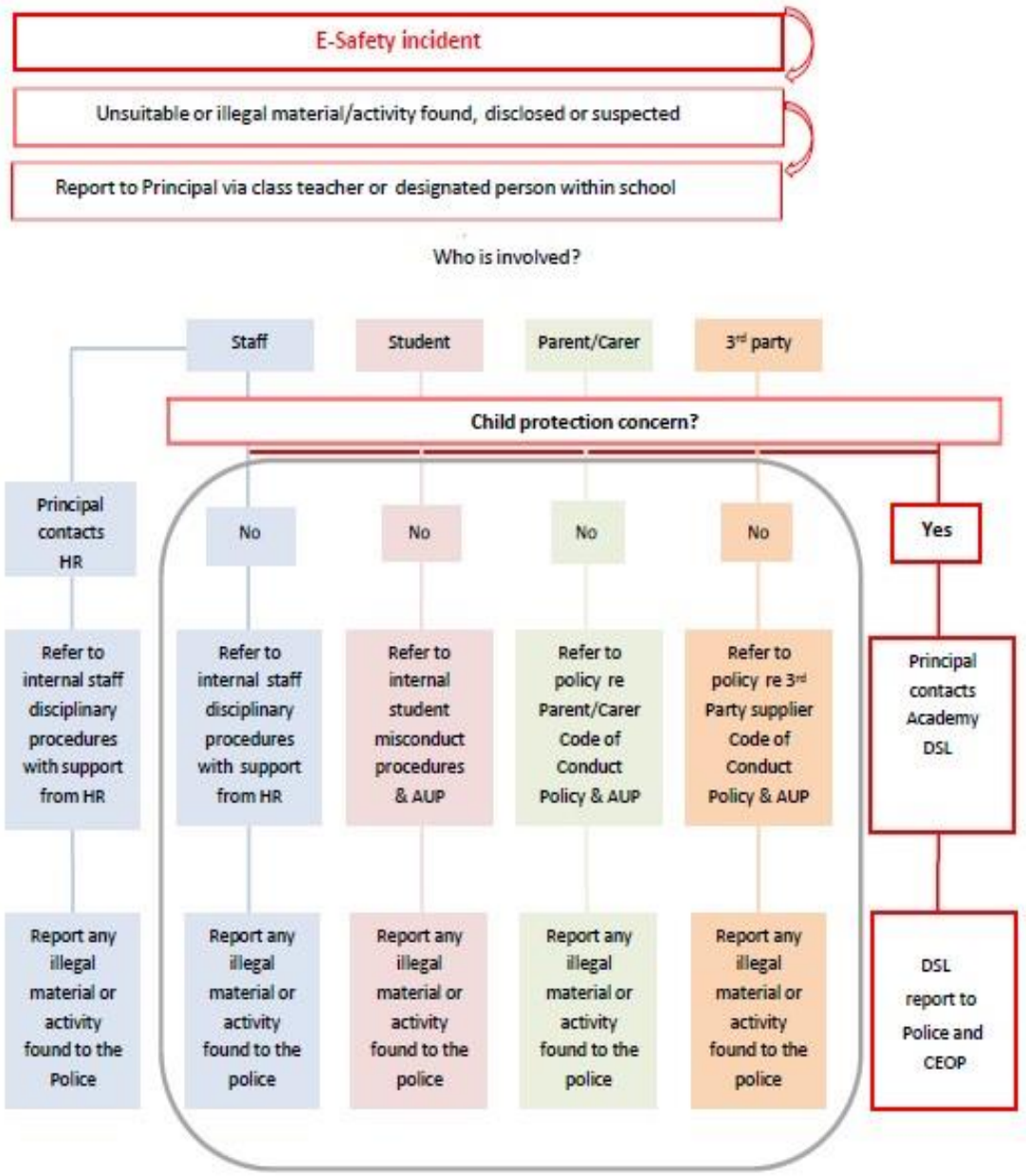
- ✓ Oasis will be checking your user area regularly to ensure correct and appropriate usage;
- ✓ you have a responsibility to use the facilities in an appropriate manner;
- ✓ you are totally responsible for your own user space **AND** any unsuitable material found in your user area is your responsibility;
- ✓ 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

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

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** |
|---|
| *Students are expected to:* |
| 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). |
| *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 lessons** |
|---|
| *Students are expected to:* |
| 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. |
| *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. |
| 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** |
|---|
| *Students are expected to:* |
| 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*** |
|---|
| *Students are expected to:* |
| 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** |
|---|
| *Students are expected to:* |
| 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** |
|---|
| *Students are expected to:* |
| 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** |
|---|
| *Students are expected to:* |
| 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). |

| *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 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.

The Academy will:

XXXX can gain maximum benefit we invite you to agree to

- 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.

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

## 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:

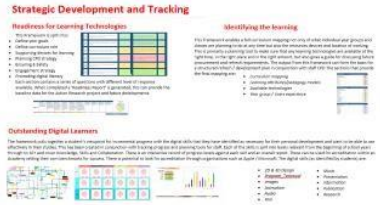
- **Learning, Sharing Productivity Tools**
- **Creativity Tools**
- **Strategic Development and Tracking**
- **IT National Challenges**
- **Accreditation Routes**

### 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:

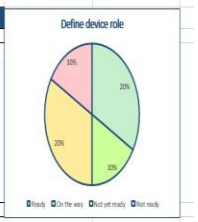
- Define your goals
- Define curriculum role
- Supporting devices for learning
- Planning CPD strategy
- Ensuring E-Safety
- Engagement strategy
- Promoting digital literacy

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 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *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* |
| **Recommended Actions** | 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**<br>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<br>Animation<br>Images<br>Presentation | Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content<br>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<br>iPads - accelerated reader sessions<br>Digital Toolkits - camera, audio recorder, tripod, mini tablet device | 42 | iMovie<br>MovieMaker<br>Photostory3<br>Purple Mash<br>Audio App - Audacity<br>Garage Band - iPads |
| Term 3 Timing TBC | **Geography**<br>'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<br>Presentation<br>Research<br>Publication<br>Audio<br>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<br>Use sequence, selection, and repetition in programs; work with variables and various forms of input and output<br>Design, write and debug programs that accomplish specific goals..... solve problems by decomposing them into smaller parts | Laptops<br>iPads<br>Digital Toolkits - camera, audio recorder, tripod, mini tablet device<br>Lego Robot kit | 42 | •iMovie<br>MovieMaker<br>Photostory3<br>Purple Mash<br>Audio App - Audacity<br>Garage Band - iPads<br>Ideas for research into geology;<br>http://www.sciencekids.co.nz/geolog<br>l |
| Extras | • Unpredictable access levels to the network / internet from within the room – some days can take 20 minutes to resolve the issues<br>• Same mismatch of versions of things on devices used by teachers students<br>• Need to know that students can access same Apps and websites, seem to be inconsistency between what | Add in:<br>2D and 3D Design<br>Music<br>e-Safety<br>Developmental logic<br>Computational thinking | Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs<br>Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems;<br>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<br>Digital Toolkits - camera, audio recorder, tripod, mini tablet device<br>Control devices - sensors etc | | Computational thinking / Developmen<br>logic:<br>https://eraseallkittens.com/en/play/<br>(works best on Chrome) ; https://code<br>Sample problems and free courses (vic<br>lesson plans etc);<br>https://groklearning.com/ straight for |

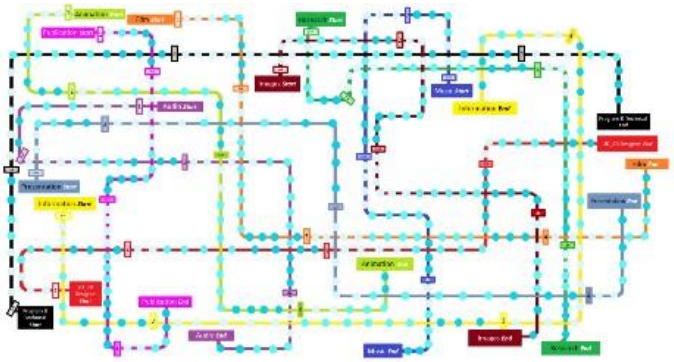
are planning to do at any time but also the resources devices and

**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.

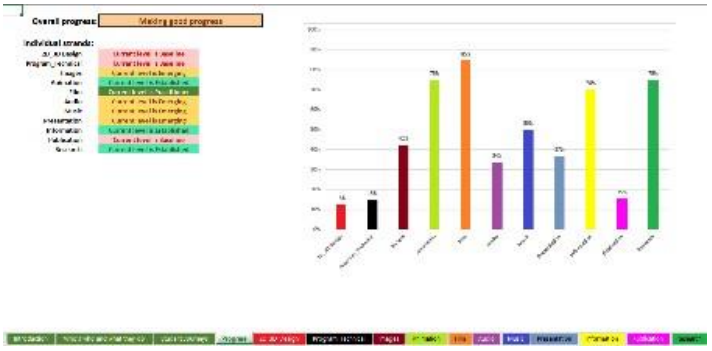
There is an interactive record of progress levels against each skill and an overall report. These can be used for accreditation within an Academy setting their own benchmarks for success. There is potential to look for accreditation through organisations such as Apple / Microsoft.



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 AUTP. 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 AUTP 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.

**Curriculum Policy (Secondary)**

*Curriculum Principles*

- 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.
- Access to the use of personal devices to allow students to develop as autonomous learners will become increasingly important within the learning environment. As IT services continue to develop, it is important that permission for the use of such devices is granted in accordance with the agreed principles of the E-Safety Policy.
- E-safety guidelines, will be adopted or adapted by the Academy. Users of the Oasis IT systems will be able to work safely if they follow the guidelines both within the Academy learning environment and their everyday life.

*Procedures*

- Students will be able to study from any location; online Oasis systems and Microsoft Office 365 will deliver a series of technology learning tools and resources to help students to plan, collaborate, and receive feedback from teachers or other expert sources that may include the use of video conferencing between sites, relating to their chosen subjects.

*Key Stage Three*

- Students will also have access to a range of technological tools to develop their own strategies for learning, sports and ICT. Religious Education may be delivered as a discrete subject or in an extra- curricular manner.

*Key Stage Four*

- Students will be able to study from any location; online Oasis systems and Microsoft Office 365 will deliver a series of technology learning tools and resources to help students to plan, collaborate, and receive feedback from teachers or other expert sources relating to their chosen subjects.

*Post 16 Study*

- Students will be able to study from any location; online Oasis systems and Microsoft Office 365 will deliver a series of technology learning tools and resources to help students to plan, collaborate, and receive feedback from teachers or other expert sources relating to their chosen subjects.

**Teaching and Learning Policy (Secondary)**

*High quality learning is the result of all teachers:*

- Being able to use a range of technological tools to aid planning, communication, collaboration and feedback

*Outstanding teaching occurs when teachers…*

- Support students in selecting appropriate technological tools to improve their development as autonomous learners
- To achieve this, Middle leaders will be expected to:
- Ensure that a wide range of technological tools are used appropriately to enhance pedagogy
- Review how effectively the students are working within the e-safety guidelines that form part of the AUTP
- Review whether the Academy's disciplinary sanctions, with regards to access to technologies, is protecting individual students sufficiently and not affecting the way in which they choose to work.
- Ensure that any external agencies, third party suppliers or other organisations working with Academies are aware of the e-safety guidelines and the AUTP
- Make sure that any incidents, either misuse of systems or access to undesirable internet websites is reported according to the Acceptable Use of Technologies Policy.

*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 online Oasis systems and Microsoft Office 365 to celebrate, share and learn from one another. The tools provided within the online Oasis systems and Microsoft Office 365 give a secure way for students to engage in a controlled social network
- ensure that students know how to protect themselves as they become autonomous users of technology systems that fall outside of the controlled Academy environment.
- Make sure that any incidents, either misuse of systems or access to undesirable internet websites is reported according to the Acceptable Use of Technologies Policy.

*Support staff will be expected to:*

- use a range of technological tools as agreed with the class teachers
- make sure that any incidents, either misuse of systems or access to undesirable internet websites is reported according to the Acceptable Use of Technologies Policy.

*Students will be expected to:*

- ensure that any devices provided by Oasis for their personal use are brought in to the Academy unless specifically told not to and are fit for purpose.
- develop safe ways of working within the e-safety guidelines from the AUTP when making use of technological tools both in the Academy and when accessing resources remotely
- understand how important the reporting any inadvertent access to undesirable internet websites or images is and ensure that they report any such instances to their class teachers • Parents and carers will be expected to:
- ensure that any devices provided by Oasis for their child's personal use are used in accordance with Oasis's Home Use Agreement Policy and are maintained fit for purpose.
- ensure that that child can work safely within the E-Safety guidelines according to the Acceptable Use of Technologies Policy.
- We believe learning will most effectively take place when:
- students select appropriate technological tools to support their learning by enabling them to plan, celebrate, collaborate and communicate in a format that is most appropriate to their own learning strategies
- See Lead Practitioner handbook guidance for planning lessons (supplementary sheets)
- Feedback
- High quality feedback improves self-motivation of students resulting in maximising their learning outcomes. Therefore, we will ensure that:
- feedback can be accessed from any location through the online Oasis systems and Microsoft Office 365 enabling students to benefit by being able to assimilate the content of feedback whenever they want/need to and wherever they are.

*Learning environment*

We believe that…

- stimulating resources through the online Oasis systems 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
- Therefore, we will ensure that…
- All classrooms are visually stimulating and designed to motivate learning and that displays:
- To ensure the safety of personal 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
- The Quality Mark: Behaviour for learning – (Optional – see Appendix E)
- Several specific policies which relate to particular aspects of teaching and learning will be developed alongside this document and will provide more specific guidance in certain areas

**Parental/carer's 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 XXXXXXX. 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 |
|---|---|---|---|---|
| 6.0 | 18/09/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updated E-Safety policy to meet new template |
| 7.0 | 28/09/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updated post Policy Meeting 26.09.17 |
| 7.2 | 21/10/2017 | | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updated post Policy Meeting 02.10.17 |

| | | | | |
|---|---|---|---|---|
| 7.3 | 31/10/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updated and reformatted biometrics and Appendix 10 |
| 7.4 | 03/11/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updated with cross references to other policies and amended parental consent/information, mobile phones statements |
| 7.6 | 24/11/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updates with references to other Policies, BYOD, Microsoft Office 365 Apps and revised Appendices |
| 7.7 | 12/12/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Updates to reflect other policies and RACI amended |
| 7.8 | 19/12/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Re-formatted and updates to reflect other policies and RACI amended |
| 7.9 | 20/12/2017 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont, Mark Thornton, Rowland Cordery, Adam Turner, Shalin Chanchani | Final draft version for editing by Rob L |
| 8.0 | 20/06/2018 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont | Revised for additional content re sexting |
| 8.1 | 21/06/2018 | Amended by Data Protection Officer, Sarah Otto | Rob Lamont | Editing |
| 9.0 | 02/07/2018 | Amended by Director of Information Technology, Rob Lamont | Philip Beaumont | Revised to include guidance on Mobile Phone Usage |
| 9.1 | 04/07/2018 | Amended by IT Project Consultant, Liz Hankin | Rob Lamont | Revised to include responses to comments and new Operational ESafety Manual Template |
| 9.2 | 14/07/2018 | Owned by IT Business Relationship Manager, Marc Hundley & Amended by IT Project Consultant, Liz Hankin | Rob Lamont | Checked for consistent use of Must and Should in line with KCSiE |

**Policy Tier**

☒ Tier 1

☐ Tier 2

☐ Tier 3

☐ Tier 4

**Owner**

IT Business Relationship Manager

**Contact in case of query**

marc.hundley@oasisuk.org

**Approvals**

This document requires the following approvals.

| Name | Position | Date Approved | Version |
|---|---|---|---|
| Phillip Beaumont | National Director of Academies | 15/11/18 | 9.2 |
| | Safeguarding Steering Group | 15/11/18 | 9.2 |
| | | | |
| | | | |

**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 |
|---|---|---|---|
| Policy Portal | | 21/11/2018 | 9.2 |
| Via: National Bulletin | | 21/11/2018 | 9.2 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |