OCL E-Safety POLICY

OASIS IT SERVICES

Last updated: 01/09/2016
Version 2.0

Document Control

Changes History

Version	Date	Amended by	Recipients	Purpose
2.0	01/09/16	Rob Lamont Head of IT	All Oasis staff	Updated Legislation

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
John Barneby	Acting Director HR	01/09/16	2.0

Distribution

This document has been distributed to:

Name	Position	Date	Version
All Oasis Academy Principals	-	02/09/16	2.0
All Academies Staff And Oasis Centre Staff	Deputy Principal	09.09.16	2.0

CONTENTS

E-Safety Policy

Introduction

Purpose

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

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

Scope

The policy applies to activities taking place 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 PCs and devices on Oasis premises.

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 SharePoint.

The contents of this document are fully compliant with the DfE statutory guidelines that come to be enforced from 05.09.2016 in 'Keeping children safe in education'. Although still under the advisory provision, the Appendices within this document and the E-Safety policy cover the use of Oasis IT Services if applied correctly within Academies.

Change

This policy is maintained by Oasis Group IT Services. Requests to change the policy should be made to the Head of Group IT Services. All changes will need to be approved by the Head of Group IT Services and the Oasis Group Executive.

Authorisation

In order to use ICT facilities at Oasis a person must have been issued staff, student or guest access to the network. Use of Oasis ICT facilities will be deemed to be acceptance of the terms and conditions of this policy.

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.

Privacy and Monitoring

Oasis IT Services reserve the right to monitor email, telephone and any other electronically-mediated communications, whether stored or in transit, in line with relevant legislation.

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.

Reasons for such monitoring include the need to:

- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of group telecommunications systems and ensure compliance with this policy or other Oasis policies;
- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);
- Prevent breach of the law or investigate a suspected breach of the law, the Oasis polices or contracts;
- Monitor standards and ensure effective quality control.

Monitoring may involve:

- Examining the number and frequency of emails;
- Viewing sent or received emails from a particular mailbox or stored on any server;
- Examining logs of ICT facility usage;
- Monitoring the amount of time spent on the Internet;
- Internet sites visited and information downloaded.

Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken. Where disclosure of information is requested by the police, (or another law enforcement authority) the request should be directed to the Head of Group IT Services or other designated staff member.

Oasis staff who have access to personal data, (as defined under the Data Protection Act 1998) 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.

Oasis IT Services maintain the right to access the Oasis email account of staff members after termination of employment for operational reasons and for the continuing delivery of services.

Definitions of Unacceptable Usage

Unacceptable use of computers and network resources may 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
- 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 actually 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

These restrictions should be taken to mean, for example, that the following activities will normally be considered to 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 store, 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 the purpose of copying unlicensed copyright software, music, etc.
- Copying of other peoples' website material without the express permission of the copyright holder
- Use of peer-to-peer and related applications. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA

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.

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 sample matrix for student-related incidents which could occur can be seen in the Oasis E-Safety Policy.

Legal constraints

Software may not be copied, installed, or used on Oasis IT equipment except as permitted by the owner of the software and by law. Oasis IT services will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license

It is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software provided by Oasis IT Services may only be used as part of the user's duties as an employee or student or for educational purposes.

The user must abide by all the licencing agreements for software entered into the by the Oasis Trust with other parties, noting that the right to use any such software outside Oasis premises will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under an Oasis agreement must then be removed from it, as well as any Oasis owned data.

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;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Criminal Justice and Public Order Act 1994;
- Trade Marks Act 1994;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;
- Communications Act 2003;
- Criminal Justice and Immigration Act 2008.

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.

For further information please contact the National IT Service Desk: servicedesk@oasisuk.org

Overview of E-Safety

Oasis recognises that the use of ICT is expanding rapidly in all sectors of society. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial. However, the internet is vast and unregulated, and, in common with all communication media, there remains the concern that it can be abused. Therefore this policy sets out strategies for the safe and responsible use of any online Oasis system and Microsoft Office 365, Oasis networks and the internet.

All users are accessing the internet both in and out of the Oasis network. Therefore, Oasis Trust aspires to ensure that all users in the Academies are aware of potential risks and how to practise safe, responsible behaviour whenever and wherever they are online.

We 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. As a consequence, when they use technology that is new to them, they will act in a responsible and safe way.

We want all professionals to use technology to enhance their working practice and find new ways of personalising learning that suit the different aptitudes and interests of learners, including those with special needs. Technology can improve the planning and delivery of teaching as well as making the learning experience more dynamic and interactive. ICT can help to ensure that students find the learning process more meaningful, enjoyable and engaging. Therefore, we want the effective use of technology to be embedded in teaching and learning across all Oasis activities.

E-Safety is seen by Oasis as an extension of general safeguarding and child safety. Therefore we aim to generate a wide-ranging awareness of the responsibilities, policies and procedures around child safety. Safeguarding users is everyone's responsibility therefore these regulations apply to all users, no matter what their role within Oasis.

This policy gives provides guidance for safe, responsible behaviour whilst accessing the Oasis systems and the internet. Please refer to the Oasis IT Security Policy and the Acceptable Use of Technology Policy for guidance regarding the security of data and ICT equipment.

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. Therefore, this policy aims to give guidance on how this can be accomplished.

Statement of Responsibilities for E-Safety

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

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 in Appendix 3 – Roles and Responsibilities

Oasis Trust Group Executive:

Overall responsibility for the E-Safety Policy

National/Regional Academy Directors:

Responsible for the effective operation and monitoring of the E-Safety Policy by Academies and Academy Councils

Oasis Academy Councillors:

Responsibility for ensuring that the E-Safety Policy is approved and applied within an Academy

Oasis Academy Principals, Senior Leaders and Safeguarding Officers

Responsibility for implementation of the E-Safety Policy within an Academy and reviewing on a regular basis

Oasis National, Regional and site-based IT support teams:

Responsibility for the creation of a safe working environment and reviewing regularly procedures against new technologies

Oasis staff, including external agencies

Responsibility to make sure that they and students can work safely within E-Safety guidelines

Oasis Students

Responsibility for their own actions and their use of IT facilities at Oasis.

Responsibilities of Parents/carers

Responsibility for understanding the Oasis E-Safety guidelines and ensuring that their child works within those E-Safety guidelines.

Each individual is responsible for making sure that they understand what their role and responsibility entails,

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

(See the Oasis Safeguarding Statement of Intent – Appendix 4)

Access to the Oasis Network, Internet, any online Oasis system and Microsoft Office 365

Oasis views access to its technology and to the internet as a privilege and not a right. Oasis's computer network is the property of Oasis and all staff have the responsibility to use Oasis' computer resources and the internet in a professional, lawful and ethical manner.

Where authorised by their line manager, staff will be provided with access to Oasis' computer network and any other access to online Oasis resources. They will be given a unique authorised user account and password for use on the Oasis Network only when they have signed and agreed to abide by the E-Safety Policy for Staff.

Parents/carers will be asked to sign and return a consent form before students are allowed to use Oasis' computer systems to access the internet or to use email facilities.

Students will be provided with access to Oasis's computer network in their initial core IT lesson. They will also be given a brief induction and explanation of their responsibilities regarding technology in Oasis. They will be asked to sign a contract agreeing to the E-Safety Policy.

Once users have signed the E-Safety Agreement (default level documents of each type of consent form is found in Appendix 5– Sample Acceptable Use Agreements) the Oasis IT Service team will be responsible for setting up authoriseduser accounts on the network and giving every user an initial password. Any passwords generated for use by the Oasis IT Service team should be changed immediately after initial use. Please see guidance on passwords below.

Oasis is committed to reinforce responsible use of the internet at every level. Therefore, 'Rules for Students', a responsible use statement which clearly states what is acceptable and what is not acceptable, should be displayed prominently wherever IT equipment and the internet is available within Oasis. (Please refer to a sample statement in *Appendix 2 – Rules for Students)*.

Passwords

With the advent of increasingly sophisticated password cracking programs, steps need to be 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.

- For staff and Students (Key Stage 3 and above) passwords must be at least 7 characters long and should be a combination of letters and numbers
- For younger students a simpler password is allowed but must be at least 4 characters long.
- 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.
- Any passwords generated for use by the Oasis IT Service team should be changed immediately after initial use.
- User accounts are issued by the Oasis IT Service team for individual use only.
- Accounts and passwords must not be shared, given away or offered for use to anybody else.
- Users must take all reasonable steps to keep their passwords confidential and must not disclose them to anyone else.
- Passwords should be changed at regular intervals.

Internet Access

All access to the internet at Oasis must be via the filtering software installed by Oasis. This filtering software should 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 in the 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 revised to block the site.

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

There is a huge amount of information available to users via the internet, and students should be taught to be critically aware of the materials they read 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.

Acceptable use of the internet is detailed in the E-Safety Policy. As a general rule, users should remember that they are acting as a representative of Oasis and should at all times have regard for Oasis policies and legislation when using the internet.

Email

Oasis operates an organisation-wide email system; where appropriate, staff and students will be provided with a unique Oasis account for their individual use. Access to this email account will be rescinded on termination of employment and all other network passwords changed

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 should not be considered private and Oasis reserves the right to monitor email accounts. To maintain the safety of staff and students, it is the policy of Oasis Trust to filter incoming and outgoing emails for viruses and potentially harmful attachments.

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 self-regulating to a large extent.

If an offensive email is received, the Oasis IT Service team or a person responsible for ICT at the Academy should 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.

Email sent to an external organisation from Oasis should be written carefully. Personal email or messaging whilst in the course of 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.

Media Publications

Video and photographic technologies can be very powerful learning tools. However, photographs and/or video may be taken by staff to support educational aims only. Named images of students will only be published with the separate written consent of their parents or carers. Publishing includes, but is not limited to:

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

Students will be allowed to use video conferencing functionality within a controlled educational context under the guidance of Oasis staff

Care should be taken when capturing photographs, videos or using video-conferencing to ensure that all students are appropriately dressed and permissions gained from parents and carers in line with normal guidance.

This may be altered or amended at any time by the parent or carer by written request.

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

Social Networking sites, Newsgroups and Forums, Chat and Instant Messaging, Personal Website and Blogs

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.

As part of the E-safety sessions run within the curriculum, 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 should protect their personal information.

Oasis will maintain online Oasis systems and Microsoft Office 365, to enable staff, teachers, students and parents/carers to jointly celebrate, share and learn from one another. The tools provided within any online Oasis system and Microsoft Office 365 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.

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.

Child protection, incidents and sanctions

Each Academy is responsible for setting in place a robust and secure system to ensure that any incidents or infringements of the E-Safety Policy are to be reported and dealt with according to their chosen discipline and sanctions policy. This should reflect how the E-safety issues will also impact upon other disciplinary policies.

To ensure a baseline of care the following areas should be clearly identified within each Academy's Policies:

- How any breaches of the E-Safety Policy will be dealt with;
- How E-Safety training will be implemented for the different users, including Parent/Carers;
- How the Acceptable Use of Technologies Agreements will be explained, issued and signed by the different users of the Oasis system and equipment.

To assist in the development of an individual Academy's policies, guidance documents have been developed with a step by step approach to:

- Roles and responsibilities
- E-Safety guides for students
- Child protection, incidents and sanctions checklists
- Acceptable Use of Technologies Agreements (See the Acceptable Use of Technologies Policy)
- Home Use Agreement (See the Acceptable Use of Technologies Policy)
- Flow diagram of how to report incidents

Appendices - Guidance documents

To support an academy in determining how to apply the E-Safety Policy and to adapt to their own environment a series of Guidance documents are provided for consideration.

The Guidance documents cover:

- Appendix 1 – Legal constraints
- Appendix 2 - Developing E-Safety, Academy Strategy for use of Technologies, Escalation points and sanctions
- Rules for Students
- Whole school planning and procedures Incidents and Sanctions Matrices
- Appendix 3 - Roles and responsibilities
- Appendix 4 - Oasis Safeguarding Statement of Intent
- Appendix 5 - E-Safety embedded in other Oasis Policies
- Anti-bullying Policy Behaviour for learning Policy Curriculum Policy (Primary)
- Teaching and learning Policy & Guidance (Primary) Curriculum Policy (Secondary)
- Parental/Carer’s Code of Conductt Policy   Offsite activities and educational visits Policy

Appendix 1

Legal constraints - references

Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally, under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

Computer Misuse Act 1990

This Act makes it an offence

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998

Oasis Trust has a comprehensive Data Protection Policy, of which the following statement is the summary:

> Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat it in an appropriate and lawful manner.
>
> The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, stakeholders and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.
>
> This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action
>
> Oasis Community Learning and the academies it manages and maintains believe that protecting the privacy of our staff and pupils and regulating their safety through data management, control, and evaluation is vital to both academy and individual progress. The academies collect personal data from pupils, parents, and staff and process it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.
>
> We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the academy will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the academy needs. Through effective data management we can monitor a range of academy provisions and evaluate the wellbeing and academic progression of our academy body to ensure that we are doing all that we can to support both staff and students.

Human Rights Act 1998

This Act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the Oasis Trust, important human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The Oasis Trust, together with all users of its IT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Freedom of Information Act 2000

The Act, intended to increase openness and transparency, obliges public bodies, including Educational Institutions, to disclose a wide range of information, both proactively and in response to requests from the public. The types of information that may be have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore all staff have a responsibility to know what information they hold and where and how to locate it.

Communications Act 2003

This Act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

Criminal Justice and Immigration Act 2008

This Act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations 'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage, but failed to take reasonable steps to prevent the contravention.'

Appendix 2

Developing E-Safety, Academy Strategy for use of Technologies, Escalation points and sanctions

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.

When mapping out students' experience for the use of a range of technological tools:

Internet	
	What are the restrictions placed on internet use within Academy?
	Are there individual logins to all accessible websites and security time-outs?
	Does the Academy use a safe list of websites, or is access filtered?
	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?
	What is 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 via group or individual addresses?
	If students do have an individual email address in the Academy, what are the restrictions on use? For example, can it be used for work-related correspondence only or for personal use? Is 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 Academy's network?
Webmail	
	What is the Academy's policy on webmail services? Are they blocked on the Academy's network?
	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?
	Spam and spoofing
	Are students aware of the issues surrounding spam and spoofing?
	Are students taught appropriate strategies for recognising and dealing with spam?
	Are technological systems employed 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 chat rooms permitted within the Academy? If so, is this for classroom use only?
Instant Messaging	
	Is access to instant messaging services 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 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 and other portable devices

	Are students aware of the safety issues relating to mobile phones and other portable communications devices, such as personal iPads, Tablet PCs and laptops? Risks include always being accessible (and hence exclusion from other forms of social contact), inappropriate and unsolicited contact by text message, text overuse and misuse, and bullying by mobile phone.
	Are students 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?
	Do students know 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 mobile phones permitted within the Academy? If mobile phones are permitted in the Academy, does the Academy provide guidelines on how and when they can be used?
	What are the sanctions for misuse?
	If mobile phones are not permitted within the Academy, how will the policy be enforced?
Camera phones	
	Are students aware of the safety issues relating to camera phones, for example having their photograph taken without their knowledge or permission?
	Are camera phones permitted within the Academy? If camera phones are permitted in the Academy, does the Academy provide guidelines on how and when they may be used?
	What are the sanctions for misuse?
	If camera phones are not permitted within the Academy, how will the policy be enforced?
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?

Whole Academy Planning and Procedures

Planning checklist for E-Safety procedures:

When formulating Academy-wide procedures:

	Does the Academy have a suite of up to date E- Safety procedures that comply with the Oasis Acceptable Use for Technologies Policy?
	Who is responsible within Oasis for E-Safety procedures?
	Are all users familiar with the Oasis E-Safety Policy?
	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 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?
When formulating support for staff E-Safety procedures	
	Do staff receive information and training on E-Safety and new emerging technologies on a regular basis?
	Is training directed to their particular 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 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?

When mapping out student experiences for the use of technologies in Oasis:

	Are students given an opportunity to contribute to Academy E-Safety procedures?
	Are students and their parents/carers provided with a copy of the Oasis E-Safety Policy 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 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?

Peer-to-peer networks

	Is access to peer-to-peer services 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 – that is, who can see what, when and for how long?
	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?

Incident and sanctions matrices

Sample - Child protection guidelines

In accordance with common child protection guidelines and to help to devise a structure for what should/could happen if there are incidents of misuse the following matrix provides guidance ensuring that users shall not visit internet sites, make, post, download, upload, transfer data, communicate or pass on material, remarks, proposals or comments that contain or relate to:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images	▨	▨	▨	▨	
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation	▨	▨	▨	▨	
Adult material that potentially breaches the Obscene Publications Act	▨	▨	▨	▨	
Criminally racist material in the UK	▨	▨	▨	▨	
Pornography	▨	▨	▨		▨
Promotion of any kind of discrimination	▨	▨	▨		▨
Promotion of racist hatred	▨	▨	▨		▨
Threatening behaviour, including promotion of physical violence or mental harm	▨	▨	▨		▨
Any other information which may be offensive to colleagues or breaches of integrity of the ethos of Oasis or brings Oasis into disrepute	▨	▨	▨		▨
Using Oasis systems to run a private business	▨	▨	▨		▨
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Oasis IT Services section and/or Oasis	▨	▨	▨		▨
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without necessary licensing permissions	▨	▨	▨		▨
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)	▨	▨	▨		▨
Creating or propagating computer viruses or harmful files	▨	▨	▨		▨
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	▨	▨	▨		▨
Receipt or transmission of materials that infringe the copyright of another person or infringes the Data Protection Act	▨	▨	▨		▨
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping/commerce					
File sharing					
Use of social network sites					
Use of video broadcast sites, e.g. YouTube, Vimeo					

Planning tool - Sanctions Matrix

Incidents of misuse and sanctions

The following matrix provides a clear indication of what sanctions will generally apply within Oasis:

	Refer to class teacher/tutor	Refer to Head of Department /Head of Year/ Other	Refer to Principal	Refer to Police	Refer to technical support team for action (filtering/security	Inform parents/carers	Removal of network internet access rights	Warning	Further sanctioning, e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal									
Unauthorised use of non-educational sites during lessons									
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									

Default Oasis IT Services policy re communication technologies

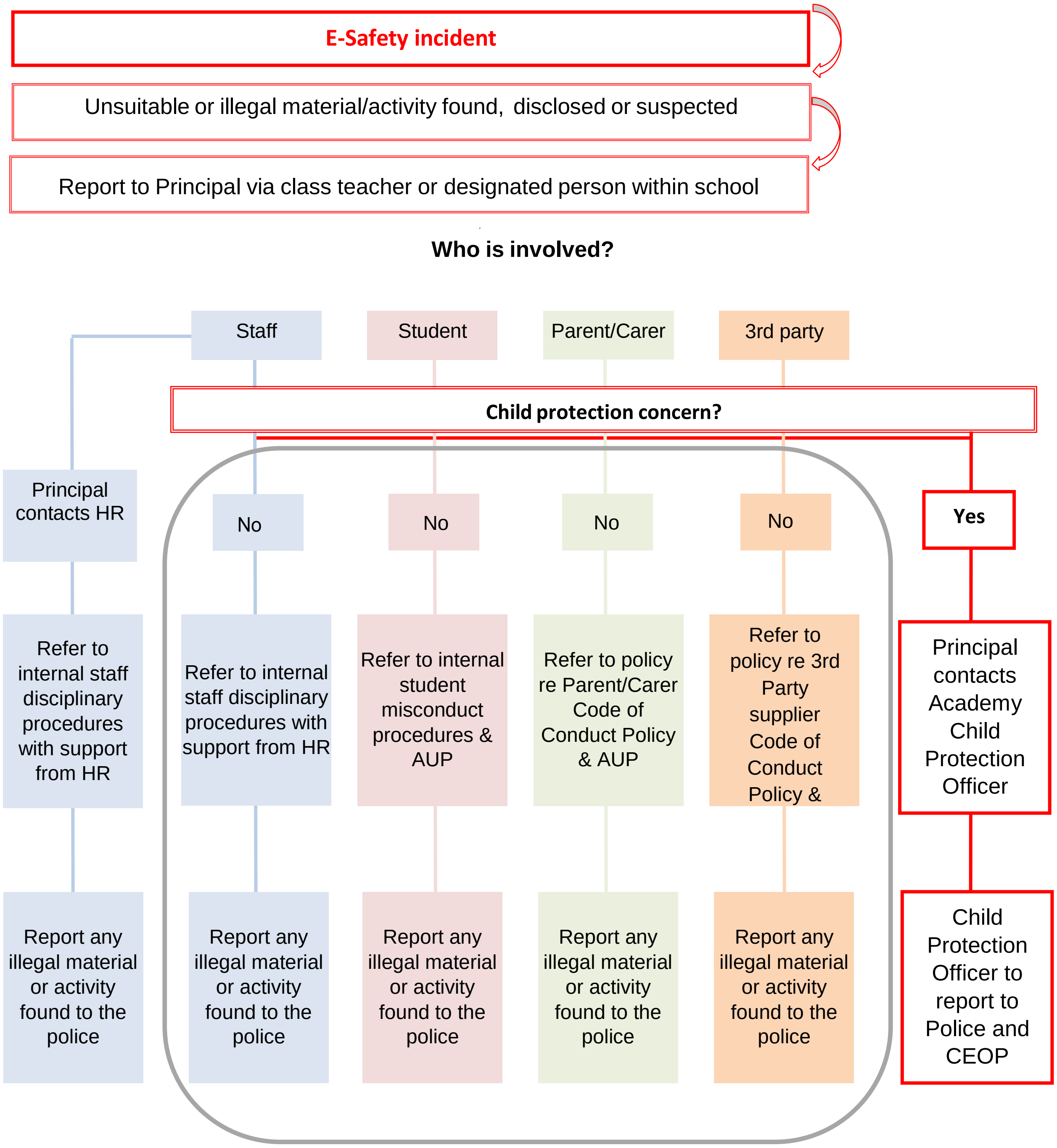
The following table shows a range of communications technologies that have the potential to enhance learning:

The list will evolve as the curriculum policy develops but an early indication of how Oasis's currently consider the benefit of using these technologies for education and the risks/disadvantages attached to their use. An Academy can provide explanations to support any contentious areas of use.

	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
Mobile phones may be brought in to Academy								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on devices with inbuilt cameras								
Use of other personal devices (PSP)								
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, etc.)								
Use of social networking sites								
Use of blogs								
Use of devices provided by Oasis during lessons								
Use of personal devices during lessons								

.

Flow diagram of how to report incidents



E-Safety incident

Unsuitable or illegal material/activity found, disclosed or suspected

Report to Principal via class teacher or designated person within school

Who is involved?

Staff

Student

Parent/Carer

3rd party

Child protection concern?

Principal contacts HR

No

No

No

No

Yes

Refer to internal staff disciplinary procedures with support from HR

Refer to internal staff disciplinary procedures with support from HR

Refer to internal student misconduct procedures & AUP

Refer to policy re Parent/Carer Code of Conduct Policy & AUP

Refer to policy re 3rd Party supplier Code of Conduct Policy &

Principal contacts Academy Child Protection Officer

Report any illegal material or activity found to the police

Report any illegal material or activity found to the police

Report any illegal material or activity found to the police

Report any illegal material or activity found to the police

Report any illegal material or activity found to the police

Child Protection Officer to report to Police and CEOP

Appendix 3

Roles and responsibilities

This Appendix outlines the roles and responsibilities for the E-Safety Policy implementation within Oasis.

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).

Responsibilities of Oasis Trust Group Executive:	
The Oasis Trust Group Executive:	
	Has responsibility for ensuring that the 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 personal 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
National/Regional Academy Directors	
The National/Regional Academy Directors	
	Are responsible for ensuring for 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
Oasis Academy Councillors	
Members of the Academy Council:	
	Are responsible for the implementation of the policies and guidance documents relating to the use of personal learning devices within an academy and for reviewing the effectiveness of the policies and guidance within Oasis.
	Will receive regular information about E-Safety incidents and monitoring reports
	Will have a nominated single point of contact for all aspects of E-Safety within the Academy
	Will regularly monitor the effectiveness of the filtering and change control logs
Oasis Academy Principals, Senior Leaders and Safeguarding Officers	
Oasis Principals, Senior Leaders and Safeguarding Officers	
	Are responsible for the day to day implementation of the policies and guidance documents relating to the use of personal learning devices within Oasis
	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 regularly monitor the effectiveness of the filtering and change control logs
	Will ensure that all staff, external agency personnel, students, parents/carers have completed the relevant Acceptable Use Agreements
	Will ensure that the Incidents and misuse matrices is adhered to by all users.
Oasis National, Regional and site-based IT support teams	
Oasis National, Regional and 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 in order 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
Oasis staff, including external agencies	
Oasis staff, including external agencies:	
	Have signed an Acceptable Use Agreement relevant to their role and responsibility
	Are responsible for ensuring that they have an up to date awareness of current E-Safety matters according to the Acceptable Use for Technologies Policy and the current Academy policies and guidance documents relating to the use of personal learning devices
	Report any incidents of misuse of the network systems or personal learning 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
Oasis Students	
Oasis Students:	
	Have signed an Acceptable Use Agreement. Parents/Carers could be expected to sign on behalf of a Reception/KS1 student)
	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.
Parents/carers	
Parents/carers will	
	Have signed an Acceptable Use Agreement for their child's use of the Oasis systems within their home or remote locations
	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 out of the Academy and realise that Oasis's E-Safety policy covers their child's/children's actions using personal learning devices outside of the Academy
	Understand that Oasis has a specific 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.
	Appreciate that according to the Acceptable Use Agreement they could be held liable for any misuse of a personal learning device outside of Oasis

Appendix 4

Oasis Safeguarding Statement of Intent

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 Health 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.

Policy and Procedures

All policies and procedures in respect of safeguarding children are up to date and 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.

Board of Trustees Responsibilities

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

Oasis is a member of the local Safeguarding Children Boards of each Local Authority in which it operates. Any issues related to safeguarding children will be discussed at these Boards each quarter.

Disclosure & Barring Checks

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.

Safeguarding Leads/Child Protection Officers

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.

Training

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. The last training strategy review occurred in December 2012.

Audit

Oasis has robust audit checklist to assure 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.

Appendix 5

E-Safety embedded into other Oasis Policies

Introduction

The overarching policy document, Acceptable Use of Technologies, has been developed to cover all aspects for the use of IT within Oasis. Following a review of the existing Acceptable Use of Technologies Policy (AUTP) 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.

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 Guidelines are provided as an Appendix to the E-Safety Policy and encourages 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:

1. Anti-bullying Policy
2. Behaviour for learning Policy
3. Curriculum Policy (Primary)
4. Teaching and learning Policy & Guidance (Primary)
5. Curriculum Policy (Secondary)
6. Teaching and Learning Policy XXXX – XXXX (Secondary)
7. Parental/Carer’s Code of Conduct Policy
8. Offsite activities and educational visits Policy

1 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

2 Behaviour for Learning Policy

4 The Academy Council's Policy on Rights and Responsibilities

4.1 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.

4.2 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.

…..

4.4 The Academy expects students:

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

……

4.6 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.

3 Curriculum Policy (Primary)

Objectives

To realise our aims our curriculum must:

12. 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.

4 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 Acceptable Use of Technologies Policy. *(See AUTP, Section 5, E-Safety; Page 9, Appendix 4, Roles and Responsibilities, Page 27 and Appendix 5, Oasis Staff Agreement Page 29).*

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.

Links with other policies and documents:

- Acceptable Use of Technologies Policy

Guidance

Acceptable Use of Technologies Policy and Appendices 1 - 11

5 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 Acceptable Use of Technology Policy (AUTP).

E-safety guidelines, forming part of the AUTP, 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.

4 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.

5 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.

6 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.

6 Teaching and Learning Policy (Secondary)

2 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

3 Outstanding teaching occurs when teachers:

- Support students in selecting appropriate technological tools to improve their development as autonomous learners

4 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. (See AUTP, Section 5, E-Safety, Appendix 4, Roles and Responsibilities and Appendix 5, Oasis Staff Agreement)

5 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(See AUTP, Section 5, E-Safety, Appendix 4, Roles and Responsibilities and Appendix 5, Oasis Staff Agreement)

6 **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 (See AUTP, Section 5, E-Safety, Appendix 4, Roles and Responsibilities and Appendix 5, Oasis Staff Agreement)

7 **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

8 **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. (See AUTP Appendix 5,)
- Ensure that that child can work safely within the E-Safety guidelines according to the Acceptable Use of Technologies Policy. (See AUTP, Appendix 5)

9 **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) Acceptable Use of Technologies Policy and Appendices 1 – 11

11. 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

12. 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

13. The Quality Mark: Behaviour for learning – (Optional – see Appendix E)

A number of 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

Add

Acceptable Use of Technologies Policy

7 Parental/carer's Code of Conduct Policy

2 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

6 Information for parents

Parents/carers will be expected to comply with the Acceptable Use of Technologies Policy and any Home Agreement that Oasis issues regarding their child's use of the online Oasis systems and Microsoft Office 365 and Academy owned equipment.

9 Guidance documents

Acceptable use of Technologies Policy Appendix 5 Acceptable Use Agreements

8 Offsite Activities and Educational Visits Policy

5.9 E-Safety procedures

- **Personal devices**

Oasis Acceptable Use of Technologies Policy applies 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.

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**