Oasis Blakenhale E-Safety Policy

September 2018

Written in accordance with the OCL E-Safety Policy July 2018

Contents

1. Academy strategy for the use of Technology

1.1 Vision for use of technologies

“Healthy bodies, healthy minds, promising futures in technology”

1.2. Procedures for use of Technologies around the Academy

Academy procedures for Incidents, escalation points and sanctions

Levels matrix of acceptable and unacceptable use

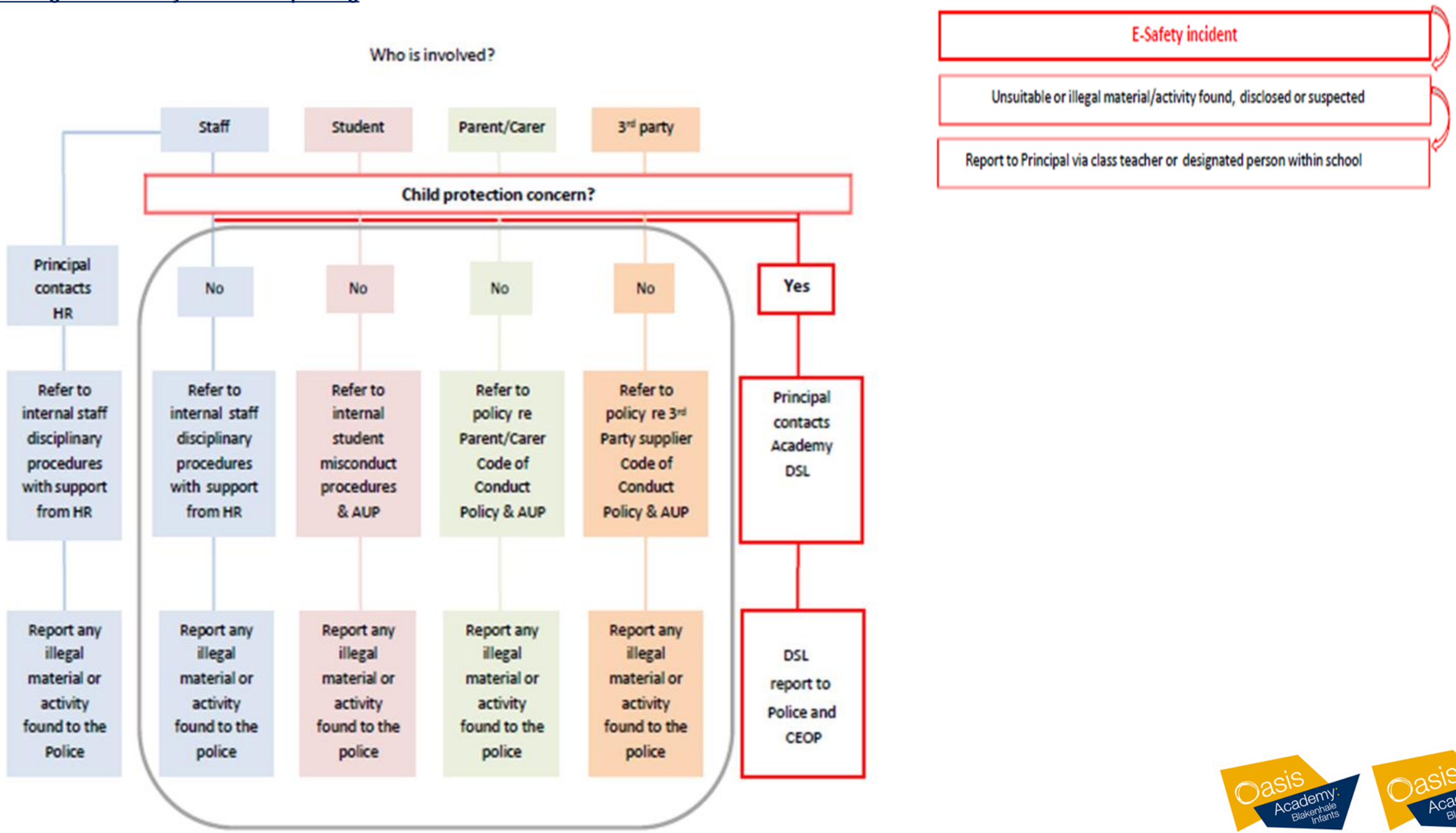
	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal	Acceptable
Child sexual abuse images						
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation						
Adult material that potentially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

1.3 Academy procedures for Incidents, escalation points and sanctions

Levels matrix of acceptable and unacceptable use

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal	Acceptable
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 gambling						
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						
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)						

1.4 Flow Diagram E-Safety incident reporting



2.0 Acceptable use of Technologies Agreements

2.1 Guidance - Use of technologies around Oasis Blakenhale

2.2 Acceptable Use of Technologies Agreements – Oasis Staff

2.3 Acceptable Use of Technologies Agreements – Oasis Students

2.4 Parent/Carer information and Opt-in Form

2.1 Guidance - Use of technologies around Oasis Blakenhale

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.

During assemblies and lessons where devices will not be used
Students are expected to:
Devices are stored in the safe secure storage trolley.
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure 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 devices are damaged by any play activities.
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.

2.1 Guidance - Use of technologies around Oasis Blakenhale

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.

In remote locations, including home environment, work placements, colleges
Staff, Teachers, TA and External Agency personnel are expected to:
Ensure students are complying with the Student Acceptable Use Agreement and if any misconduct is identified apply the correct level of discipline/sanction.

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.

2.1 Guidance - Use of technologies around Oasis Blakenhale

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.

Before the Academy day starts
Students are expected to:
Take any personal device (mobile phone) straight to the academy office, to be locked in the academy's safe, and collected at the end of the day.
It is the students responsibility to take and collect their personal devices from the academy office.
A parental request must be made if they want their child to bring a mobile phone into the academy (permissions are usually granted to Year 6 pupils who have permission to walk home without a parent at the end of the day)

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.

2. Acceptable use of Technologies Agreements

2.2 Oasis Staff

Acceptable Use Policy (AUP): Staff

Name of Academy: **Oasis Blakenhale Infants and Oasis Blakenhale Juniors**

AUP review Date:

Date of next Review:

Who reviewed this AUP

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.

2.0 Acceptable use of Technologies Agreements

2.2 Oasis Staff

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.

2.0 Acceptable use of Technologies Agreements

2.2 Oasis Staff

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.

Signature …… Date ……

Full Name …… (printed)

Job title . . . . . .

Academy . . . . . .

Authorised Signature (Deputy Principal)

Signature …… Date ……

Full Name ……(printed)

Confirmation signature (Executive Principal)

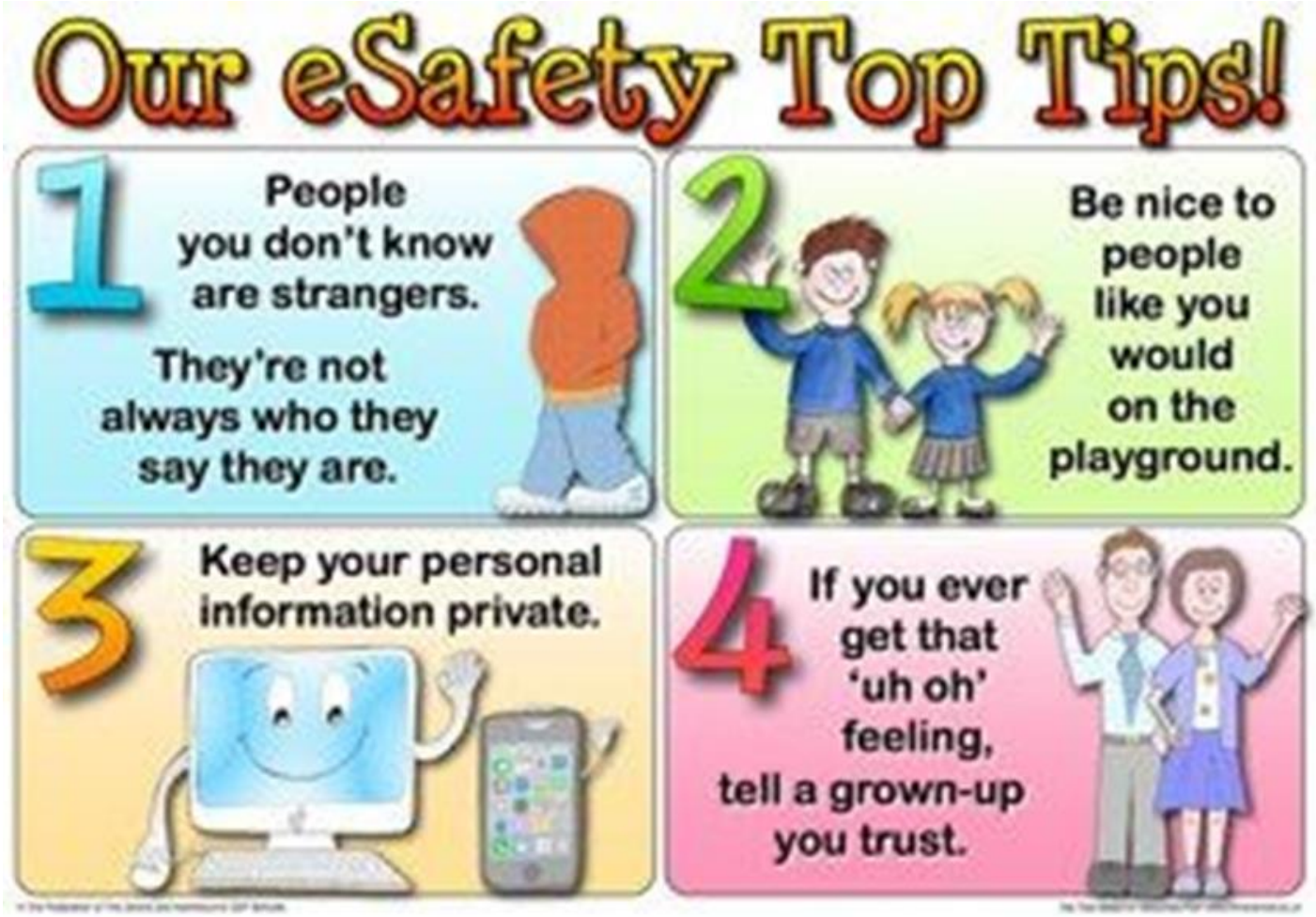
Signature …… Date ……

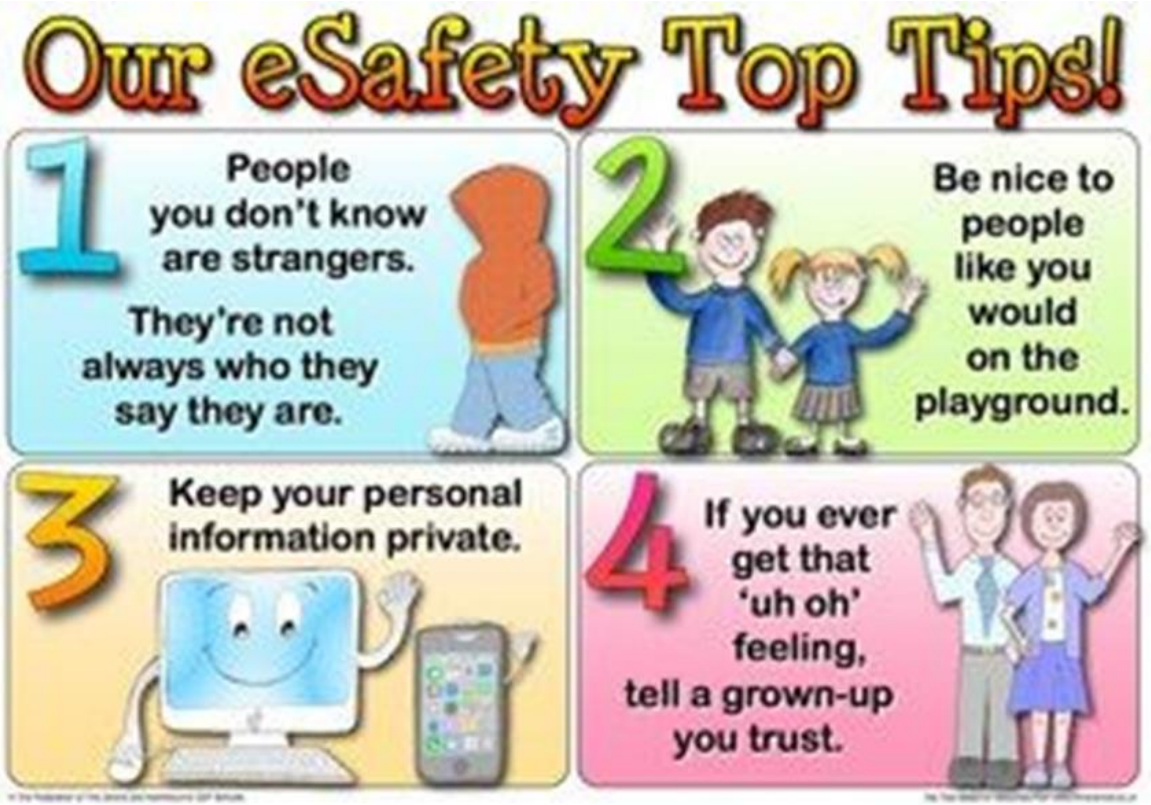
Full Name …… (printed)

2.3 Acceptable Use of Technologies Agreements – Oasis Students

Guidance – Age appropriate agreement discussion & Rules for Students

Key Stage 1





Class <name>

We agree to follow the IT (Information Technology) rules at Oasis Blakenhale Infants.

Pupil's signatures

Terms and Conditions – Acceptable Use of Technologies Agreement (Key Stage 2 only)

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.*

Terms and Conditions – Acceptable Use of Technologies Agreement (Key Stage 2 only) continued…

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.

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.

Rules for Students (Key Stage 2)

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.

Rules for Students (Key Stage 2)

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.

I …….. have read and agree to follow the rules for using IT (Information Technology) at Oasis Blakenhale Juniors

Signed: …… Name: ……

3.0 Whole Academy Operational E-Safety matrix and sanctions

3.1 Operational procedures

At Oasis Blakehale we ensure that all E-Safety operational procedures comply with the Oasis E-Safety policy including the Acceptable use of Technologies and use of personally owned devices. All stakeholders are consulted when policies are being reviewed or re-written. Using the overarching Oasis E-Safety policy has a basis for ours, we consult and take input from; pupils, teaching staff, technical support staff and the Academy Council. The policy is then finalised by the ALT. All staff and pupils who access the technologies are responsible for E-Safety operational procedures but ultimate responsibility falls to the DSL's and finally the Executive Principal. Staff will always have access to E-Safety Policies and the Academy Operational E-Safety document. Time is allocated throughout the academic year to highlight key areas from the policies, this make take the form of a staff briefing, a professional development meeting or an INSET day. For an Academy Councillor, a dedicated section in meetings will always be allocated to Safeguarding (including E-Safety).

E-Safety rules differ in the Infants and Junior academy's, In the Infant academy, there are four clear and simple internet rules, which are shared with the pupils every half term and displaying in all classrooms. In the juniors the rules are more comprehensive and pupils need to sign an acceptable use policy to acknowledge they have understand and will comply to these rules. Within the rules pupils are aware of the reporting procedures; infant pupils are taught to report any images that give them a 'uh oh' feeling to report it to a grown up while junior pupils are taught to report any aggressive or inappropriate behaviour directed at anyone, including themselves. Staff are also aware of how to report incidents (see Academy procedures for Incidents, escalation points and sanctions), alongside this there is a reporting flow chart displayed in the staff room.

E-safety does not apply solely to the Information Technology, the importance of it is highlighted in many of the other academy policies including;

- Safeguarding (KCSIE 2016)
- Behaviour for learning
- Curriculum policies
- Teaching and Learning Policies
- Anti-Bullying Policy

Clear and robust systems have been set up and applied for the misuse of Oasis IT systems and equipment (see sanction matrix). Pupils are informed through the behaviour policy of consequences. Staff are made aware through briefing sessions, access to the E-safety policy and through continued professional development meetings. The Oasis E-Safety procedures and reports are reviewed annually in accordance with the OCL policy, changes will be made within an academic year if current polices do not reflect government guidelines.

3.2 Operational E-Safety staff support

At Oasis Blakenhale staff are receiving information and training in E-Safety and new emerging technologies on a regular basis. E-Safety forms an important section in the annual Safeguarding training at the beginning of each academic year where staff are reminded of the procedures and sanctions within the policy. Particular attention is drawn to the acceptable use policy, which staff read, and sign to acknowledge the expectations within and outside the academy.

Staff training is directed to their specific role in the Academy, although E-Safety training will mostly encompass all staff members. Materials published by the NSPCC and ThinkUKnow website are used to support staff in E-Safety development; this includes the completion of online training modules provided by the NSPCC for key members of staff.

There are clear processes for staff to report any difficulties or concerns they may encounter (see procedures for Incidents, escalation points and sanctions section for more information). Any member of staff new to the academy have direct access to the E-safety policy, and are shown the Academy operational E-safety part of the document and must sign the acceptable use policy.

When using any form of Information Technology within the curriculum, E-safety must play an integral part of the planning process for staff. Curriculum maps contain a safeguarding section which highlight the E-safety elements that will be covered. Staff are expected to incorporate E-safety activities and awareness into all lessons that contain an IT element. Staff are expected to be vigilant during lessons and to report any misuse. Whole school monitoring is carried out regularly through the Future Clouds monitoring system by the designated safeguarding lead.

When newer technologies are introduced to the academy, information and training on E-Safety, play a crucial part in this process.

Staff will receive annual training on information literacy skills so for example they are able to search validity of information effectively. More information about information literacy can be found on the following website: https://infolit.org.uk/

3.3 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

At Oasis Blakenhale we have a student safeguarding team. The pupils meet half termly to discuss potential safeguarding issues, whereby they can contribute to the safety (e.g. the pupils have a greater understanding of the E-safety rules for acceptable use, and can reinforce them in lessons with their peers). Parents have access to this policy through the academy's website.

When pupils begin at our academy (aged 2 or 3 if they join in Nursery; 4 or 5 in Reception), they have little or no experience of technologies – most will be able to use a tablet or mobile phone. At Oasis Blakenhale we want the pupils to have greater keyboard skills and know how to use technologies safer so in the EYFS (Early Years and Foundation Stage) we aim to ensure achieve this.

All four E-safety rules are displayed in classes, and all pupils (except Nursery) will have half termly E-safety assemblies. In addition to this Key Stage 1 pupils sign to say they will use the technologies safely. Overview have been created to ensure all e-safety elements are covered each academic year (some sessions are kept free in case of any urgent updates on the Think U Know website are published. All assemblies link to the acceptable use whilst at school and at home – pupils are sign posted to responsible adults if they are exposed to anything whilst online at home (this includes signposting them to the NSPCC/Child Line).

E-safety links are discussed at the beginning of all lessons which use newer technologies – this may be a brief synopsis of the rules or a more in depth talk depending on the need for safe use of technologies (e.g. Year 2 email pupils from Zimbabwe so a bigger emphasis on e-safety will be delivered by the class teacher for this unit of work, whereby if they are accessing a trusted app on the iPads then a reminder about use it safely will suffice).

Pupils understanding of E-Safety issues are measured annually, with pupils in Key Stage 1 completing an online form (Microsoft), pupils rate (using a 5 star rating) how safe they feel when they are using IT in the academy and at home.

3.4 Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Internet
The academy uses a monitoring program called Future Clouds, to restrict access to websites. Any inappropriate web pages are flagged up to the DSL who will then add the website to the restricted ones through Future Clouds. Children are taught from the beginning of Reception to inform a responsibile adult of any content that makes them feel uncomfortable, this can also be reported through the DSL and restrictions can be placed to these websites. Alongside this, a report is sent to the DSL/E-safety lead bi-weekly, within this report it lists a number of key words that have either been typed or screen shot. The DSL will randomly select some of the hits from this report to identify if there has been any misuse, if the content is harmless it is recorded in a record has a false positive. If there is malicious intent then the DSL will follow the academy's procedures for incidents.
The Academy does not restrict the use of websites to a safe list due to the vast range of educational websites available to pupils, although staff need to plan any lessons carefully when using the internet, checking the content and appropriateness to the age range they delivering lessons to.
The IT system does not allow children to download content from the internet, lessons are planned carefully to allow children to access the key resources needed to meet the objectives to specific lessons. Due to the potential and hiddent risks to the IT system all types of materials are prohibited from downloading.

Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Email

Currently children do not have access to email within the academy, although further developments in the Year 6 IT curriculum are developing to include a unit of work on emailing. This will initially be restricted to OCL academies. Planned unit of work will look at covering the following areas; using appropriate language, attachments to emails, identifying SPAM and phishing emails, recognise and reporting incidents of bullying and the consequences to email misuse. The aim of this unit of work is to get pupils secondary ready and to be able to use email safely.

Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Webmail

Children do not use webmail services within the academy although we recognise the importance of using such services outside the academy safely. As part of a unit of work in Year 6 pupils will learn about webmail services safely outside the academy. As part of this unit of work students will know how to use the following features; using inbuilt junk mail filters, understand the viruses surrounding spam and spoof, identify and deal with spam email. The aim of this unit is to get pupils secondary school ready and to be able to use webmail safely.

Chatrooms

Children are not permitted in the academy to access chatroom – these sites are blocked through our monitoring system. Although within our acceptable use policy and E-safety assemblies – children are taught how to identify online bullying and to report anything that makes them feel uncomfortable to a responsible adult.

Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Instant Messaging

Currently pupils do not have access to instant messaging services. If a decision is made for students to have access, further lessons will be introduced to ensure pupils protect personal information and know how to keep safe. The instant messaging would be restricted to closed groups or buddy lists. Pupils will be taught how to seek help or advice if encountering any issues or problems.

Mobile phones/portable devices

The academy only allows personally owned devices/phones for Year 6 pupils and in some circumstances Year 5. Any child who is given permission must bring their device into the school office at the beginning of the day. This is then locked in the school safe by a member of the administration team. It is then the child's responsibility to collect their device/phone from the academy office at the end of the day. Personal phones/devices are not permitted in lessons or around the academy.

.

Operational E-Safety student access to technologies

Decisions about student access to and use of technologies within academy

Webcams

Currently webcams are not used within the academy for curriculum activities. Pupils are taught of the dangers of using a webcam through internet safety lessons or assemblies, and how to report any concerns or threats they may receive.

Decisions about student access to and use of technologies within academy

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?

Peer-to-peer networks

Peer-to-peer services are not used within the academy, and the filtering system will block

any such services. If for any reason the filtering system will block any such service.

3. Academy procedures for Incidents, escalation points and sanctions

3.1 LEVELS MATRIX OF ACCEPTABLE AND UNACCEPTABLE USE

	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					

Academy procedures for Incidents, escalation points and sanctions

3.1 LEVELS MATRIX OF ACCEPTABLE AND UNACCEPTABLE USE

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 gambling					
On-line shopping/commerce - Academy decision (Exception – Finance office with signed purchase order from Executive Principal)					
File sharing – (Acceptable through OneDrive)					
Use of social network sites – (Twitter only – using the Academy's account)					
Use of video broadcast sites, e.g. YouTube, Vimeo – (Can be used in lessons but it is the class teacher responsibility to check the content of the video before showing to the pupils, and then it **must** be viewed in safe mode).					

3.2 SANCTIONS MATRIX

	Refer to class teacher	Refer to year group leader	Refer to Deputy Principal	Refer to Police	Refer to technical service desk but inform IT Cluster Manager	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									

3.2 SANCTIONS MATRIX

	Refer to class teacher	Refer to year group leader	Refer to Deputy Principal	Refer to Police	Refer to technical service desk but inform IT Cluster Manager	Inform parents / carers	Removal of network / internet rights for fixed period of time	Warning	Further sanctions e.g. detention / exclusion
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									

3.3 Academy decisions re use of communication technologies

Oasis Blakenhale's 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 (educational only e.g. TES)								
Use of instant messaging (e.g. Skype for Business, Yammer, Messenger etc.)								
Use of social networking sites								
Use of blogs								
Use of devices provided by Oasis during lessons								
Use of personally owned devices during lessons								
Academy policy allows students to have personally owned mobile phones/mobile devices with them in school								

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.

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

Risk Register with related concerns and implications for the use of technologies within Oasis Blakenhale Academy

E-Safety Risk Register

						Low (1) Medium (2) High (3)		RAG	Date	Open / Closed
No.	Owner	Other Contributors	Detail	Aspect	Migration	Likelihood	Impact	Final		
1	CC	Finance/ OCL Finance/ IT	Under –funding and obsolescence of IT resources. Lack of investment leads to reliability and security issues, plus accumulation of long term maintenance backlog reduces flexibility, reduces project quality, increases upgrade times and generates unpredictability	Ensure clear action plans are in place and costs of future spending is pre-planned. Work with IT team to ensure 'old' equipment is identified for refresh	Sinking fund – if detrimental to IT infrastructure	1	3	3	09/18	Open
2	CC	IT team	Loss of key personnel. Many systems are understood by only one person, who could leave, become ill, have an accident etc. Some systems could then be difficult to maintain, with extended down-time, or projects could be delayed.	Ensure when new systems are introduced at least two members of staff have the training. When a lead is nominated ensure another member of staff has responsibility to cover this responsibility in the absence of the lead.	Ensure named person - who will stand in if key personnel are absent	2	3	6	09/18	Open
3	CC	IT/finance	Software licensing changes. Software supplier could withdraw licenses for vital items, significantly change the price, go out of business, sell rights etc. Affect costs and ability to provide items widely. Risk prosecution if unaware.	Work closely with the IT team with software development – ensure only software that is approved by the MAT is deployed in the academy.	Give written notice to cancel software licensing	1	2	2	09/18	**Open**
4	CC	IT Team	Failure of applications software, e.g. triggered by incompatibility due to changes in related systems or by increased demands. This could lead to unavailability of particular services and possible extra costs.	Cloud based software – back-up in place if the network goes down. IT regularly carry updates on all machines. Support desk to be contacted immediately in the event of an application failing.	Back up – checked regularly	2	2	4	03/19	Open
5	CC	Data Protection team IT Team	Changes to systems required by legislation, or new requirements from funding bodies. Possible requirements to stop using existing process if not planned ahead.	Constant attention to and understanding of legislation. Information Security Officer in place. PCI/DSS compliance being addressed.	Report any breaches immediately	1	3	3	**09/18**	**Open**
		IT Team	Outsourced services (including Microsoft and Apple).	Careful checking of third-party services	Report any					

5 Academy Risk Register

Risk Register with related concerns and implications for the use of technologies within Oasis Blakenhale Academy

E-Safety Risk Register

						Low (1) Medium (2) High (3)		RAG	Date	Open / Closed
No.	Owner	Other Contributors	Detail	Aspect	Migration	Likelihood	Impact	Final		
7	CC	IT Team	Internal fraud or sabotage. Disgruntled or untrained staff could do enormous damage to IT systems and data.	Ensure all staff understand and sign the terms of the AUP. Staff complete training annually on E-safety (completed in Microsoft Forms).	See reporting matrix	1	3	3	10/18	**Open**
8	CC	IT Team	Unauthorised access to computers and data.	A Code of Conduct for all computer users, including version and change management. Good documentation of procedures and dependencies.	See reporting matrix	1	3	3	09/18	**Open**
9	IT Team		Failure of backup systems. This would destroy the security of data making it vulnerable to many other risks.	IT have systems in place to automatically back up data, if there is a failure to back up data the IT team will be informed where they will carry out a manual back-up and address any issues.	Restart system	1	3	3	09/18	**Open**
10	IT Team		Virus or other malware attack, or software vulnerabilities. Malicious software can damage any IT system, or prevent normal service by sheer volume of extra traffic.	All stakeholders at the academy are aware to report any phishing emails (staff informed of how these can be presented when sent). Use of high-quality virus/malware detection regularly updated on all devices.	Shut down system	1	3	3	09/18	**Open**
11	CC	IT Team	Loss of telephone connection. This would disrupt all normal voice communication, and would be a major problem in an emergency such as fire.	Fire procedures in place – practised termly. Use of mobile phones in place if phones lines do go down. Listed emergency numbers easily accessibility.		1	3	3	09/18	**Open**
12	CC	IT Team	Theft of vital equipment, or associated damage. Targeted theft of IT equipment has occurred on three occasions in the past 5 years.	Computer suite and iPads physically secure. Higher risks of iPads being stolen due to security of certain rooms.	Report to police	2	3	6	09/18	**Open**

5.0 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 Blakenhale. 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)
Oasis Data Protection Policy
Oasis IT Security Policy
Oasis Acceptable Use of Technologies Policy
Oasis Use of Personally Owned Devices Policy (UPOD)

6.0 OCL Safeguarding

At Oasis Blakenhale 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 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. The policies are accessible through the academy's websites.

Anti-bullying Policy

'3.2 We all have responsibility to respond promptly and effectively to issues of peer to peer/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.

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

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.

Student Account Passwords

For a younger student (Reception – Year 2) 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.