eSafety Policy

(R.E.A.L. Education Ltd.)

(R.E.A.L. Independent Schools)

(R.E.A.L. Alternative Provision School)

Amended on: 10.7.19

Review Date: August 2020 or sooner in the event of an issue arising

Revision history:

Version 1	Completed Tuesday 4 March and shared with ICT working party and Nicky Bailey as Safeguarding lead for REAL Education.
Version 2	Update to What ifs section by CW
Version 3	22.12.15 Updated names and positions of key staff. Checked all areas of policy and updated where appropriate. Presented to eSafety group for approval in January 2016.
Version 4	11.1.16 Adopted policy template and style. N. Goddard
Version 5	21.12.16 Annual review and update by Craig Wilkie Minor updates to social media section. Minor updates to What if section.
Version 6	23.5.18 Annual review and update by Craig Wilkie Updated policy to reflect GDPR Updated emerging technologies section to ensure ICT Strategy group and eSafety group lead on the management and implementation of projects.
Version 7	10.7.19 Annual review and update by Craig Wilkie. No major changes to the policy.

The School eSafety Coordinator (also the chair of the eSafety group)	Richard Smith (Director), supported by Craig Wilkie (ICT Services Lead)
Safeguarding leaders	Nicki Purcell, Kay Carter, Martin Davies,

	Andy Richmond

Our e–Safety Policy has been written by the R.E.A.L. eSafety Strategy group, building on the national guidance.

The policy covers all Education provision offered by R.E.A.L. including the individualised provision, R.E.A.L. Independent School, R.E.A.L. Alternative provision and activities carried out by the R.E.A.L. Foundation Trust.

A member of the working party is a CEOP ambassador and much of the policy relates to best practice as promoted by CEOP, the government's national child protection agency for eSafety.

R.E.A.L. Education's eSafety Strategy group takes responsibility for eSafety.

Policy Contents

eSafety Policy

Overall vision for eSafety
Keeping students safe is of the highest priority. Our eSafety vision is simple.

Safe to learn
We want our young people to work thoughtfully in a safe environment whilst in our care and whilst away from our care.

Safe for life
We want young people to live a safe digital life, harnessing the great opportunities which technology brings us whilst feeling empowered to make good choices to stay safe with technology.

What do we mean by technology?
Technology within this policy means electronic equipment which provides us with information. Technology is another word for ICT (Information Communication Technology)
This includes the hardware, such as laptops, tablets and ipads and desktop computers and software which are the programmes and applications which people use. Examples of software programmes include Microsoft Office tools such as Word .This definition also includes the things which are harder to see, such as the internet,computer networks including cloud services. These are types of ICT services. Throughout the policy we may use the term technology and ICT interchangeably.

How does technology benefit education in R.E.A.L.?
ICT benefits learning and teaching in the following ways:

- Provides an engaging and motivational way to learn, especially for some of our most disengaged learners.
- Allows pupils access to a rich variety of multimodal information eg. video, audio, images, text, to engage numerous learning styles and preferences.
- Allows pupils to connect to learning in accessible ways eg. by providing a writing framework or having the computer read instructions to them to support various learning needs.
- Supports high quality teaching through the use of diverse and interactive resources.
- Supports a collaborative approach to learning in a managed, structured and controlled way as a scaffold towards face-to-face collaboration, our final goal.
- Supports personalisation by providing flexibility in the pace, place and time of learning.
- Culturally enriching by connecting pupils to people and communities in different localities, opening minds and raising awareness of our cultural heritage and responsibility as global citizens.

The internet at R.E.A.L. Education

The internet can provide the following specific benefits:

- Access to worldwide educational resources.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data through our Atmos learning platform.
- Access to learning wherever and whenever convenient.
- Communication systems with up-to-date information.

How can internet use enhance learning?

- Education can happen away from school, using tools such as Atmos and Edlounge.
- Internet research, including the skills of knowledge location, retrieval and evaluation.
- Online activities that support the learning outcomes home.
- Pupils can use web based tools to collaborate on learning activities.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Copyright law will be adhered to by the school when using materials from the Internet and this will be addressed in the eSafety scheme of work.

Commitment of R.E.A.L. Education to eSafety

We are committed to improving our approaches to eSafety and keeping staff and pupils safe. We use http://www.360safe.org.uk/ to benchmark R.E.A.L.. Education against other schools nationally.

We have currently been awarded a Certificate of Commitment and Progress from the national awarding body.

R.E.A.L. Education is committed to ensuring that at least one member of the eSafety group is a CEOP Ambassador. This supports the dissemination of good practice and resources through the organisation to standards set by SOCA (Serious Organised Crime Agency) to safeguard children in the digital world.

In addition, we plan for eSafety developments through the ICT Action Plan which sets out a series of actions to improve our approach and delivery of eSafety projects and programmes in a coordinated way across R.E.A.L. Education.

The R.E.A.L. Education eSafety group

R.E.A.L. Education has an eSafety group that meets regularly throughout the year. The group owns, monitors and coordinates the delivery of improvements in eSafety. Developments from this group are detailed in the Safeguarding Action Plan. The eSafety group supports improvements across the R.E.A.L. Independent School, R.E.A.L. Alternative Provision and R.E.A.L. and personalised programmes. A cross section of staff and key leaders represent all areas of R.E.A.L. Education in the eSafety group. There is a Terms of Reference for this group.

On induction at R.E.A.L.

When pupils are inducted at R.E.A.L., they are asked to read and sign our **Guide for eSafety** (A visual **Acceptable Use Policy** form). This is their contract with us to ensure they take their responsibilities for eSafety seriously and that their parents/carers will do likewise to support us. https://docs.google.com/a/real-education.org/document/d/1Vk6YjRWwyFNHvh6zANbNq-Ma8Q_EAQE-v6c7rW_Vuic/edit

This form is checked, updated and ratified by the eSafety group on an annual basis.

Or search in Atmos for: Guide for eSafety.

In addition, parents/guardians sign the **REAL, ICT data process and storage statement, agreement for parents and pupils to give us permission to use and store information at**

R.E.A.L. Education. Completion of this agreement is a prerequisite of joining R.E.A.L. Education.

https://docs.google.com/a/real-education.org/document/d/1tVl8XysUn3juRQDhRpk9Yk2PMGselGwGr2IE2GcU1Vk/edit

This form is checked, updated and ratified by the eSafety group on an annual basis.

Or search in Atmos for: ICT data process

Both agreements need to be printed out, signed and completed, a copy provided for the parent/carer and pupils (as appropriate) to take home with them. A copy should then be returned to the central pupil file for future reference.

Managing Information

How will information systems security be maintained?

- Updating virus protection regularly.
- Regularly assessing access to a learners information through during key milestones eg. person centred planning meetings.
- The ICT service will review system capacity and security at least annually and present this to the Directors.
- User logins and passwords are required to access Atmos data storage.
- Users are required to use two step authentication to ensure access to data is secured to the highest possible levels.
- Personal data sent over the Internet, stored on our Atmos Learning Platform or taken off site will be encrypted.
- Regular, planned training and support for all staff who access information systems including an eSafety session during induction for all staff.
- Independent penetration testing of the network and systems on a regular basis.

How will email be managed?

- Staff have access to email, their responsibility is clearly identified in our REAL email etiquette acceptable use policy which is signed on induction by all staff.
- Pupils use of email is permitted with Learning Manager consent and restricted to email within R.E.A.L.. (ie. the pupil cannot email someone who does not have an @real-education.org email address.)

R.E.A.L. email etiquette, acceptable use of email

https://docs.google.com/a/real-education.org/document/d/1M6WSkXOgrYxOl-NFxUJPgWhVUIrgnHzM8eiESsTzang/edit

Or search in Atmos for: Email etiquette

How will social networking, social media and personal publishing be managed?
At induction, all staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status at R.E.A.L. Education.

In different industries, there are varying expectations around the use of social media eg. Facebook, Twitter and LinkdIn. As R.E.A.L. is an educational provider and independent school we set very high standards around responsible use of social media. This includes the use of social media in **non-work time**.

All staff have a responsibility to ensure their actions when using social media do not compromise the integrity and professional standing of themselves and R.E.A.L. Education. This applied to social media use in work time and outside of work time.

As internet sites and resources are increasingly adding a social element to their appearance and operation, staff should consider all web resources carefully and work with the ICT Service to select resources that are safe to use.

Pupil use of social media

- Where filtering is in operation, access to social media and social networking sites can be controlled by filtering software. By default social media is blocked at all venues R.E.A.L. Cloud filtered venues.
- Social Media tools used in the classroom will be risk assessed before use and planned into a scheme of work with agreement from Headteacher/Learning Manager prior to the lesson.
- Pupils will be advised on security and privacy online and concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites (see also What if? guide in appendix).
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location (as agreed at induction).

Staff use of social media

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

- Staff should not use social media to “sound off” about their day or staff/children. Social media to share anonymised teaching and learning experiences e.g. discussing resources and strategies used, is acceptable. Opinions should not relate to the school or allow a child to be identified in any way.
- Staff should refuse any contact from pupils or parents through social media. This includes ex-pupils and ex-parents.
- A good rule of thumb is to consider; How would a Director/my employer feel if this message/post was read by them?

An excellent guide for staff who use Social Media in both professional and personal life should be read:
http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals

Use of social media for communications within R.E.A.L.
At R.E.A.L.. Education we use social media to support communication and marketing activities. We adhere to the following:

- Restricting access to social media accounts only to authorised staff.
- Messages on social media relate to good news and positive achievements eg. Good News Community.
- We don’t use social media to make religious, political points or raise controversial issues.
- We respond to any criticism in a timely and positive fashion with the outcome to demonstrate our openness, transparency and desire to work in a positive and proactive way with families and organisations.
- We regularly review our communications to ensure we act and communicate in an appropriate way for the particular social media tool - in line with our corporate image and responsibility.

Use of social media for parental engagement
At R.E.A.L.. Education we use social media to support communication with parents.

The purpose of this group is to

- Build a supportive and positive community of people at R.E.A.L. Education
- Allow R.E.A.L. Education to communicate general information about opportunities that could be really useful to you and your child
- Allow parents to work together to develop ideas and share their views about projects and initiatives at R.E.A.L. Education.

Keeping social media communications positive and productive

- We use a ‘closed’ FaceBook group which is open to all current parents.

- We restrict access to official R.E.A.L. social media accounts only to authorised staff, including the parent coordinator.
- The group is monitored by the parent coordinator and at least one Director.
- All posted messages must adhere to our rules of use.
- We reserve the right to remove users who break the rules of use.
- We respond to any criticism in a timely and positive fashion with the outcome to demonstrate our openness, transparency and desire to work in a positive and proactive way with families and organisations. We remind users that this is not the forum to criticise members of staff.
- We regularly review the way we use social media to engage with parents to ensure we act and communicate in an appropriate way for the particular social media tool - in line with our corporate image and responsibility.
- We encourage a shared role of ownership and management of social media groups with parents - working in partnership to ensure the vision of social media use is maintained.

How will filtering be managed?

- Broadband access includes filtering (at some venues) appropriate to the age and maturity of pupils and the school's filtering policy will be regularly reviewed by the eSafety team, with changes being risk assessed and with consent from the SLT where appropriate.
- Chromebooks used by pupils in an independent learning scenario can be filtered to the highest standard, where access is allowed to a specific list of approved websites. The expectation is that a Learning Manager would work with the ICT Team to tailor the filtering levels for a specific pupil **prior** to them being given a Chromebook.
- Any breaches of filtering (e.g. inappropriate content) will be reported to the headteacher and logged in the SIRF form. All members of the school community (all staff and all pupils) will be aware of this procedure at induction.
- The eSafety team will meet regularly to review the SIRF and check that any necessary changes are are made to ensure that the filtering methods selected are effective.
- The school's filtering decisions will pay heed to the age and curriculum requirements of the pupils, with advice from network managers and ICT Strategy Group.
- Where pupil's access a learning location that is does not have filtered internet (this could be because the site is part of an educational visit, temporary working space etc…) consideration should be given to complete a risk assessment. Certainly, the pupil should not be left unattended with the internet, activities should be thoughtfully planned to make sure specific , relevant sites are accessed. Consideration should be made to provide a Chromebook for these instances as this provides filtered internet access from any location.

Unblocking websites that have been blocked by the filtering software

Occasionally, the filtering software blocks legitimate and safe websites which would add value to learning.

Where staff wish to unblock or gain access to a filtered website, they will log their request at www.realservicedesk.co.uk Where the website is clearly safe, the technician will unblock the site and record the decision in the ServiceDesk. Where there are concerns about a website's safety/security, the technician will discuss concerns with the member of staff. If the request cannot be resolved, the issue or request should be raised to the Headteacher/Learning Manager and ICT Services Lead for a final decision.

How will videoconferencing be managed?

- The use of videoconferencing with pupils will be planned and confirmed by the Headteacher or Learning Manager.
- The Headteacher or Learning Manager will decide if a risk assessment is necessary.
- Staff should remind the other party about house rules etc…
- Staff will never leave children unattended when a video conference is in progress.
- By default, all Google/Atmos video conference services are restricted.
- Staff will have access to Google Hang Outs, a video conferencing service provided to connect and communicate with each other. The use of this service is for professional use only in work and non-work time.
- A notice should be added to the door or the room to make it clear to anyone entering the room that a video conference is in progress and that they may appear on video.

How are emerging technologies managed?

- Emerging technology means any new ICT hardware or software innovations.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use policy.
- The eSafety and ICT Strategy group will govern and manage the trialling and adoption of all new and emerging technologies so they are formally risk assessed and consistently managed and maintained.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR. (See also the Data Protection Policy).
- All staff and parents agree on induction to our REAL, ICT data process and storage statement.

- R.E.A.L. Education will comply with freedom of information requests in accordance with Freedom of Information Act 2000 and recommendations from the Information Commissioner's Office.
- R.E.A.L. Education demonstrates this compliance by registering with the Information Commissioner's Office that we process personal data.
- We have a Data Policy which outlines the full responsibilities and expectations of how we process and store data at R.E.A.L.

REAL, ICT data process and storage statement, agreement for parents and pupils

https://docs.google.com/a/real-education.org/document/d/1tVl8XysUn3juRQDhRpk9Yk2PMGselGwGr2lE2GcU1Vk/edit

Or search in Atmos for: ICT data process

REAL, ICT data process and storage statement for staff

https://docs.google.com/a/real-education.org/document/d/1guEtJIdGzH_ePtzrioA8JnEF_B5Ry2922rxExJuaQ6I/edit

Or search in Atmos for: ICT data process

How will Internet access be authorised?

- All staff will read and sign the following policy on induction:

STAFF: SAFE and RESPONSIBLE INTERNET USE

https://docs.google.com/a/real-education.org/document/d/1m7TrU1nQehKhrw6Z1GJUG0opXjTRigKlm9z3nYPw3gY/edit

Or search in Atmos for: Staff internet

All guests and visitors will sign and complete the form, below, before being given an wifi password to provide limited access to the internet. The access will be removed after a limited period of time.

VISITORS: SAFE and RESPONSIBLE INTERNET USE

https://docs.google.com/document/d/1-blgE4GNJta6gaWyQEfyrWicHlFkzhViwfw7SFQbNmI/edit#

Or search in Atmos for: Visitors internet

- Parents will be asked to read and sign the **Induction guide for eSafety** for pupils and discuss it with their child, where appropriate.
- All visitors to R.E.A.L.. Education who require access to the internet access will be asked to read and sign the **VISITORS: SAFE and RESPONSIBLE INTERNET USE** (this may include agreeing to these terms digitally as part of the secure log in requirements.)
- When considering access for vulnerable people (such as with children with special education or emotional needs) R.E.A.L. Education will make decisions based on the specific needs and understanding of the pupil(s) in collaboration with parents/carers. It is the responsibility of the Learning Manager to tell the ICT team if a pupil requires specific restrictions to technology eg. if their EHCP denies access to the internet.
- At Key Stage 2, pupils will be fully supervised when using the internet.
- At Key Stage 3 and 4, pupils will be supervised when using the internet, where Chromebooks have been authorised for use, the pupil will access only a small selection of websites. This gives us the confidence to allow the pupil unsupervised access. Tutors can request a web history / internet use history regularly through a Service Desk request.

How will risks be assessed?

- R.E.A.L.. Education will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, **it is not possible to guarantee that access to unsuitable material will never occur** via a school computer. R.E.A.L. Education cannot accept liability for the material accessed, or any consequences resulting from internet use.
- The school's eSafety group, in conjunction with the Headteacher and Learning Managers will regularly meet and review the eSafety policy, to ensure it is adequate and being implemented appropriately. They will identify, assess and ensure methods are in place to minimise risks.

How will the school respond to any incidents of concern?

- All members of staff will be informed about the procedure for reporting eSafety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The eSafety Coordinator and/or the eSafety group will record all reported incidents and actions taken in the School eSafety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any eSafety incidents involving Child Protection concerns, which will then be escalated appropriately.
- R.E.A.L. will manage eSafety incidents in accordance with the school behaviour policy

where appropriate. Staff to refer to 'What If' appendix for common eSafety issues (see appendix.)

- R.E.A.L. will inform parents/carers of any incidents of concern as and when required. In most cases, this will be in person, on the day of the incident.
- After any investigations are completed, the eSafety team will debrief, identify lessons learnt and implement any changes required and if necessary, contact the Area Children's Safeguarding Team and/or CEOP.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the **Anti-Bullying** policy.
- All incidents of cyberbullying reported to the school will be recorded in the SIRF log in accordance with other reporting expectations.
- Evidence will be gathered and stored before being deleted.

Sanctions for those involved in cyberbullying may include:

- Making a copy of the material as evidence.
- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at R.E.A.L. for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to other policies at R.E.A.L.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms be managed?

A Learning Platform is an secure online space for storing data and collaborating. At R.E.A.L. we use Atmos, our Learning Platform based on world-leading, Google Apps technology.

- Staff will regularly monitor the usage of the Learning Platform by pupils and staff in all areas, in particular message and communication tools and publishing facilities. Such communication tools are restricted to R.E.A.L. education staff and pupils only.
- Pupils/staff will be advised about acceptable conduct and use when using the Learning Platform, in accordance with the **Induction guide for eSafety.**
- Only members of the current pupil, parent/carers and staff community will have access to the Learning Platform, it is the responsibility for the Business Team to raise a Service Desk request to the ICT team when a member of staff leaves the organisation.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.
- When staff, pupils etc leave the school their account or rights to specific school areas will

be disabled and stored in our digital vault for as long as it is necessary, in accordance with our Data policy.

- Any concerns about content on the Learning Platform may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the Learning Platform for the user may be suspended.
d) The user will need to discuss the issues with the Headteacher or Learning Manager before reinstatement.
e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the Learning Platform by a member of the SLT. In this instance there may be an agreed focus or a limited time slot and with a risk assessment completed by SLT.
- Where a visitor/commissioner is given access to Atmos, an Acceptable Use Agreement will be signed and access to specific areas of the Drive will be provided for a limited period of time and with a risk assessment completed by SLT.

How will mobile phones and mobile devices be managed?

- The use of home-owned mobile phones, tablets, ipods etc…. and other personal devices by pupils is restricted at R.E.A.L..
- Home-owned devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity, with consent from a member of staff and authorised on each occasion by the Headteacher or Learning Manager.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Any images or video created at R.E.A.L. on a home-owned device must be deleted from the device before it is taken home.

Pupils Use of Personal Devices

- We recognise that for many pupils they are reliant on access to a mobile phone. Rather than a blanket policy covering all key stages and situations, we expect that appropriate use of mobile phones is encouraged by all staff.
- Where use of a mobile device/home own technology affects engagement in learning, appropriate responses should be taken in accordance with the behaviour policy.
- In R.E.A.L. Education, if a pupil needs to contact his/her parents/carers they will be allowed to use a school phone or the school office will contact the parent/carer for them. Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity, even after the pupil ceases to be taught at R.E.A.L. Education.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Care should be taken when using a mobile phone or device in school time so as not to compromise professional expectations. eg. even in the staff room or staff kitchen , think about who can view or hear the content from a mobile phone, could they be offended by the content? How would a Director react to viewing this content and is your professional integrity negatively impacted?
- If a member of staff breaches the this policy then disciplinary action may be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- An eSafety training programme/scheme of work will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- It is the responsibility to ensure that eSafety rules/posters/displays or copies of the pupil Acceptable Use Policy will be posted in all venues used exclusively by R.E.A.L. Education and responsible use of the Internet and technology will be encouraged across the curriculum. Rules will be adapted and presented in a way that is suitable for the age and maturity of the pupils in each class.

How will the policy be discussed with staff?

- The eSafety Policy will be formally provided and discussed with all members of staff at induction.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- The eSafety group will highlight useful online tools which staff should use with children in the classroom and at other learning locations. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The ICT newsletter will be used to promote eSafety and share best practice and

resources.
- An online eSafety course is provided for staff to access and updated annually.

How will parents' support be enlisted?

- Parent's/carer's attention will be drawn to the **Induction guide for eSafety**.
- A partnership approach to eSafety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting eSafety at other attended events e.g. parent evenings.
- Parents/carers will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Review

This policy will be reviewed annually as the nature of eSafety is rapidly changing.
What ifs...a practical guide to dealing with eSafety issues in class.
Please remember that this is not a "straight jacket" to adhere rigorously to, these guidelines will help to prompt and inform your unique response. All esafety responses should be coordinated with the Headteacher/Learning Manager as appropriate.

This guide forms part of the eSafety policy for R.E.A.L. Education.

An inappropriate website is accessed unintentionally by a pupil or member of staff.

1. Play the situation down; don't make it into a drama. Ask the pupil to turn off the monitor, minimise the web page or close the laptop lid, so the image or text cannot be seen by other pupils in the class. Make a note of the web address in the URL bar.
2. Discreetly discuss why the site is inappropriate with the pupil, or any issues that their experience might raise. Tell them who else they could talk to if what they have seen worries them eg. parent/carer, CEOP.
3. Report to the Headteacher/Learning Manager as soon after the event as is reasonably possible eg. break, lunchtime if the incident happens in the independent school (essentially this must be before the pupils concerned leave to go home). The Headteacher/Learning Manager decides whether it is appropriate to inform parents/carers of any additional pupils who viewed the site.
4. Record incident as an eSafety log and email this to the Safeguarding Lead.
5. Inform the school technician to ensure the site is filtered using Service Desk.
6. Technician informs the filtering service/filters webpage.

An inappropriate website is accessed intentionally by a pupil

1. Explain why they should not be viewing this content. Show them where to find the appropriate and relevant information they are searching for.

2. Refer to the **Induction guide for eSafety** that was signed by the pupil and parents/carers.
3. Preserve any evidence through print outs or screen capture.
4. Use the school behaviour policy to identify the line of action.
5. Inform parents/carers if necessary as this may be a pattern of negative behaviour which is going unchecked at home.
6. Inform the school technician to ensure the site is filtered if need be.
7. Technician informs the filtering service/filters webpage.
8. Record incident as an eSafety log and email this to the Safeguarding Lead.

You observe another adult using IT equipment inappropriately on school premises (eg. viewing videos on YouTube which are clearly unsuitable, posting inappropriate images of themselves on a social network.)

1. Report the misuse immediately to a member of the Safeguarding lead. Do not speculate or discuss the issue with other staff. Do not challenge the member of staff who you observed.
2. Technicians will be instructed to ensure that there is no further access to the PC or laptop (device) if the device is owned by R.E.A.L. If the device is owned by the user eg. a mobile phone, the Headteacher/Learning Manager and user of the device should negotiate how data can be obtained through the device (if appropriate), alternatively this can be obtained through the network use logs.
3. If the material is offensive but not illegal, R.E.A.L. Headteacher/Learning Manager could then:
    a. Remove the equipment to a secure place
    b. Suspend user from email and Learning Platform accounts.
    c. Instigate an audit of all ICT equipment by the schools ICT technician to ensure there is no risk of pupils accessing inappropriate materials in the school.
    d. Identify the precise details of the material
    e. Take appropriate disciplinary action
    f. Inform the designated Safeguarding Lead if material is pupil related.
    g. Refer the incidence to the Local Authority Designated Officer (LADO)
    h. Inform governors of the incident

In an extreme case where the Directors deems the material is of an illegal nature:

4. Contact the Police or CEOP and follow their advice.
5. If requested, remove the PC/equipment to a secure place and document what you have done.
6. Record incident as an eSafety log and email this to the Safeguarding Lead.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Secure and preserve any evidence using screen capture or photographing a monitor or mobile phone.
2. Inform the SLT/eSafety team who will work with the member of staff to preserve the evidence and identify the comments which are upsetting for the member of staff or pupil.
3. Inform and request the comments be removed if the site is administered externally.
4. Send all the evidence to CEOP at www.ceop.gov.uk, take guidance over the nature of the comments.
5. Endeavour to trace the origin and inform police if appropriate, applying the behaviour policy or staff conduct expectations. Refer to the Acceptable Use policy and the Staff ICT policy.
6. Record incident on an eSafety log and email this to the Safeguarding Lead.

You are concerned that a pupil's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the pupil.

1. Report to and discuss with the Headteacher/Learning Manager as soon as possible, certainly on the day of the incident and contact parents.
2. In partnership with parents/carers, advise the pupil on how to terminate the communication and save all evidence offering confidential support to do so if needed.
3. Consider taking action to report/suspend account ensuring evidence is retained, do not delete the social network account at this stage. Offer advice and direct support to parent re. setting up safe internet etc...
4. Contact CEOP www.ceop.gov.uk with parent/carer and pupil and ask for advice.
5. With the Headteachers/Learning Manager and advice from CEOP, consider the involvement of other professionals.
6. Take steps to check actions have been successful in stopping inappropriate contact.
7. Record incident as an eSafety log and email this to the Safeguarding Lead.

A member of staff overhears a conversation between two KS2 pupils. The conversation was meant to be private. One of the pupils mentions that she is meeting up with a girl tonight, who she met through a Facebook/social network group.

1. Consider that the pupil may be at risk of meeting an **adult** stranger tonight, without parental knowledge who is masquerading as a primary pupil.
2. Inform the Headteacher/Learning Manager and plan a response before the end of the school day on the day of the incident. The Headteacher and Learning Manager may decide that it is necessary to supervise the pupil until a parent/carer can be contacted.
3. Contact home to ascertain whether the parents/carers are accompanying the pupil to meet their "online" friend.
4. The pupil is under 13 and has a Facebook account, whilst this is not illegal, check that

the parents/carers are aware of this. The parents must be informed.
5. Record incident as an eSafety log and email this to the Safeguarding Lead.

A current pupil asks you to be their online friend on a social network such as FaceBook.

1. Politely decline the pupils offer and explain the inappropriateness of the request.
2. The same should also apply for online gaming, text messaging and any other forms of communication.
3. If the pupil (ex-pupil) persists in making contact with you ie. after you have declined to connect/befriend them, record incident as an eSafety log and email this to the Safeguarding Lead.
4. Record incident as an eSafety log and email this to the Safeguarding Lead.

You suspect that a pupil is accessing the school computers through the use of a staff username and log in. You have no idea how this may have happened. (This scenario is highly unlikely to occur as a pupil would need to have ownership of a staff username, password and staff mobile phone, plus mobile phone unlock PIN.)

1. If you suspect your own password has been compromised, immediately complete a Service Desk request or contact the Business Team at head office.
2. Report to the Headteacher/Learning Manager.
3. The ICT can check the history of log-ins to verify your concerns.
4. If a pupil is found to have used a staff login, remind them of the Acceptable Use Policy which they signed. Apply the behaviour policy.
5. Identify if there has been a breach of confidential data and inform the Directors, Headteacher and Learning Manager if you suspect there may be. eg. has the pupil copied and transferred data from the Staff Shared drive to their Facebook account / memory stick / mobile phone?
6. Record incident as an eSafety log and email this to the Safeguarding Lead.

You wanted to take some photos of the pupils and their work and post these on the school website to celebrate their achievement

1. Check that every pupil and family has signed and agreed to the Photograph policy consent form.
2. Take the photo with work camera (not a personal camera from home).

3. Never identify the pupil in the photo with their name, if this can be viewed by the public (eg. it will be on the website).
4. Out of courtesy, inform Headteacher/Learning Managers then the parents/carers before the image is live on the web. Do this even if you have consent to use the photo, out of courtesy to the parents/carers/pupil as their circumstances may have changed.

Useful e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Kidsmart: www.kidsmart.org.uk

Think U Know website: www.thinkuknow.co.uk

360 safe – e-safety self-review tool: http://www.360safe.org.uk/

Significant Incident form to be completed

Where there is immediate danger to a pupil
Contact the Safeguarding lead immediately by phone, contact the Business Team at R.E.A.L. if you are unable to contact the Safeguarding lead. Stress that this is a child protection issue and it is imperative that a message is received by a Safeguarding lead immediately, to make contact. Do not relay the details of the issue to anyone other than the Safeguarding Lead.

Where there is no immediate danger to a pupil
Complete an SIRF form and note eSafety as an issue:
https://docs.google.com/a/real-education.org/forms/d/e/1FAIpQLSd2onch93Cg9cxuoRIM0wfBVQ3IkLzMeqwTAeQfU5wcDe582g/viewform

eSafety long term overview, scheme of work (Draft)

Early KS2

Knowledge and understanding	Skills and responsibilities	Suggested activities
Rules help keep children safe when exchanging learning and ideas online. Understand that websites may not be accurate or reliable and can be persuasive or biased. Begin to understand that the internet contains facts and opinions. Understand the need to keep passwords safe and the importance of strong passwords. Understand that information shared using ICT can be easily copied and made public.	Identify the risks and rewards of using the internet at home and school. Know and put into practice basic eSafety rules and healthy choices eg. limiting screen time. Begin to understand the difference between copying and pasting from the internet and re-wording information in your own words. Consider when to open an email or attachment. Understand why we use an avatar or alias online. Respect others ICT work and messages. Understand that unkind messages and pictures will upset others and may constitute as bullying.	Use internet to research and gather information. Think about when we use the internet and who can help us to stay safe. Share and exchange ideas using ICT with others beyond the school eg. emailing a charity or partner school as a whole class under adult supervision. Design nicknames and avatars, begin to create a class Social Media page offline eg. , so positive attitudes towards sharing information can begin to be established. Share information between children safely eg. emailing within the class.

Later KS2

Knowledge and understanding	Skills and responsibilities	Suggested activities

Explore and discuss positive and negative impacts of ICT use at home and school. Understand the eSafety rules in school and broader rules eg. Age ratings on games, minimum age limit of social media. Understand what personal information is and why it is risky to share this with people you do not know. Understand the need to evaluate content on the internet carefully and establish reasons why people may put inaccurate information on the internet. Begin to explore internet scams such as phishing and spam and know how to respond to such threats. Understand about copyright and how to use information from the internet in a legal and respectful way.	Make good choices when using ICT, with reference to the eSafety rules. Know where to find out about eSafety eg. use of the CEOP website. Know how to stay safe on social media sites. Create and use strong passwords. Evaluate websites and the content on them, identifying any risks and how to manage these. Know they have a right to be protected from inappropriate use of ICT and a responsibility to others to respect their rights eg. when using a digital camera, requesting consent from subject.	Know the consequences of sharing information online: Use CEOP video Jigsaw. Discuss the eternal nature of content posted online and the lack of control a user has. Quote sources and respect copyright when using ICT. Consider which communication tools are most appropriate for the content, speed, audience etc… Use spoof websites such as Northwest Pacific Octopus to evaluate information on the web and discuss fact/opinion and plausibility. Use cross referencing (other websites and books) to ascertain facts.