R.E.A.L. Education Limited

Online Safety Policy

(R.E.A.L. Education Ltd.)
(R.E.A.L. Independent Schools, Ilkeston)
(R.E.A.L. Independent Schools, Blidworth)
(R.E.A.L. Independent Schools, Hinckley)
(R.E.A.L. Independent Schools, Mansfield)

Last reviewed: 12th July 2023

Contents

1. Introduction

The School online safety Coordinator	Clare Walker
Safeguarding leaders	Kirsten Gibson, Head of Schools Tracey Keeling, Head of Safeguarding and Standards

Our online safety policy has been written by the Head of Safeguarding and Standards with support from the ICT services team. The policy builds on national guidance. The policy covers all education provision offered by R.E.A.L. Education.

Keeping learners safe is our highest priority, and our policy is informed by the *Keeping Children Safe in Education 2023* guidance. Our online safety 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 whilst feeling empowered to make good choices to stay safe with technology.

The four Cs
Our strategy and practice is guided by the 4 C's:

Content - protecting our learners and helping them to make judgements about the content they access.

Contact - ensuring that contact via technology is managed, monitored and restricted as necessary.

Conduct - reminding learners how they have a duty of responsibility to themselves and others in the choices and freedoms that technology permits.

Commerce - helping learners to understand risks such as online gambling, inappropriate advertising, phishing or financial scams.

2. 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, ipads or desktop computers and software such as;

programmes and applications. This definition also includes the things which are harder to see such as the internet, computer networks and cloud services. Throughout the policy we may use the term technology and ICT interchangeably.

At R.E.A.L. Education we recognise that technologies that are not connected to the internet may also pose a risk e.g. digital cameras and tracking devices. The policy title of Online Safety is a narrow definition of technological risks however remains in keeping with the nationally understood phraseology.

2.1 How does technology benefit education in R.E.A.L.?

ICT benefits learning and teaching in the following ways:

- Provides an engaging and motivating way to learn, especially for some of our most disengaged learners.
- Allows learners access to a rich variety of multimodal information e.g. video, audio, images and text to engage numerous learning styles and preferences.
- Allows learners to connect to learning in accessible ways e.g. by providing a writing framework or having the computer read instructions to support accessibility requirements.
- 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.
- Supports personalisation by providing flexibility in the pace, place and time of learning.
- Culturally enriching by connecting learners to people and communities in different localities, opening minds and raising awareness through cultural capital.

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

The internet can provide the following specific benefits:

- Access to worldwide educational resources.
- Access to experts in many fields for learners 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 platform.
- Access to learning wherever and whenever convenient.
- Communication systems with up-to-date information.

How can internet use enhance learning?

- Internet research.
- Online activities that support learning outcomes at home.
- Learners can use web based tools to collaborate on learning activities.
- Learners are able to develop skills and competencies that will help them to take a full and active part in society and their next stage of learning, employment and adulthood.

Learners will be taught what internet use is acceptable and given clear boundaries for internet use. Copyright law will be adhered to by the school when using materials from the Internet.

4. Commitment of R.E.A.L. Education to online safety

We are committed to improving our approaches to online safety and keeping staff and learners safe. We use the LGFL Digisafe (https://national.lgfl.net/digisafe) tool to benchmark R.E.A.L. Education against other schools nationally.

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

4.1 On induction at R.E.A.L.

During the induction process learners complete an Online Safety section to support understanding of their responsibilities for online safety. Learners also sign an agreement, alongside their parents/carers to further support this.

5. Managing information

How will information systems security be maintained?

- An ICT Services policy which documents the process and policy around managing and upkeeping ICT systems and services.
- Updating virus protection regularly.
- The ICT service will review system capacity and security at least annually and report 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 online safety session during induction for all staff.
- Independent penetration testing of the network and systems.

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.
- A learner's use of email is permitted with Learning Manager consent and restricted to email within R.E.A.L. (ie. the learner cannot email someone who does not have an @real-education.org email address.)

- Expectations for email etiquette and acceptable use is outlined in guidance below.

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

How will social networking, social media and personal publishing be managed?
At induction, all staff are made aware of the potential risks of using social networking sites or personal publishing in either a professional capacity with learners or personal use. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how content may breach the staff code of conduct.

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 applies 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

- By default social media is blocked at all R.E.A.L. venues through the Cloud filtering.
- Social Media tools used in the classroom will be risk assessed before use and planned into a scheme of work with agreement from the Learning Manager prior to the lesson.
- Learners will be advised on security and privacy online and concerns regarding learners' use of social networking, social media and personal publishing sites (in or out of school) will be raised as a safeguarding concern.
- Learners will be advised never to give out personal details of any kind which may identify them and/or their location (as discussed 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 staff Acceptable Use Policy. This will include advice and support for staff to check that their security settings are appropriate .
- 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.

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. Google Spaces
- We do not engage in challenging conversations with users on social media in a public forum, but direct them to make contact with us via the phone in a private forum.
- We do not mention or share identifiable images of learners on social media unless directed to do so by the Senor Designated Safeguarding Lead.
- 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.

How will filtering be managed?

- Broadband access includes filtering (at all R.E.A.L. Education owned venues) appropriate to the age and maturity of learners and the school's filtering policy will be regularly reviewed by the online safety team, with changes being risk assessed and with consent from the ICT Strategy Group where appropriate.
- Chromebooks used by pupils in an independent learning scenario can be filtered to the highest standard using through iboss, supplied by ekte, 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 Head of Schools/Head of Safeguarding and Standards and logged in either a SIRF form, or safeguarding concern form (whichever is most relevant). All members of the school community (all staff and all pupils) will be aware of this procedure at induction.
- The ICT Strategy group will review the concerns raised through either the SIRF form, or safeguarding form and check that any necessary changes are made to ensure that the filtering methods selected are effective. The statistics and agenda for these conversations is led by the Head of Safeguarding and Standards and recorded in the minutes of the ICT Strategy group. The purpose of this activity is to ensure that the Safeguarding lead is being supported with the ICT team's technical professionals to ensure systems are protecting staff and students.
- There is regular reporting to the Governors of any breaches and subsequent actions taken.
- The school's filtering decisions will pay heed to the age and curriculum requirements of the learner, with advice from the ICT team and ICT Strategy Group.
- Where learner's access a learning location that 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.

- Where the filtering service is disrupted at one or more venues, the Safeguarding lead and Directors will be informed immediately. By default, the recommendation will be to stop using the internet until the filtering can be re-activated.

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

- Provide the ICT support team with 72 hours notice to unblock a website.
- Check with their Deputy (site lead) first to gain consent to unblock a site.
- Log their request at www.realservicedesk.co.uk confirming consent and the name of the senior leader.

There are separate arrangements for unblocking and blocking content at the Digital Creative site. This is due to the 'industry' standard environment. The provision lead, Neil Kellow, is responsible and accountable for the decisions made around filtering provision.

Where the website is confirmed as acceptably 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 Head of Schools or Deputy (site lead). If the request cannot be resolved, the issue or request should be raised to the Head of Schools/Learning Manager and ICT Services Lead for a final decision.

The senior leader making a decision is doing so on the understanding that the website is being unblocked for all users at that site/location. The senior leader takes full responsibility and accountability for the decision they make.

6. How will video conferencing be managed?

Video conferencing is an alternative for specific 'face to face' meetings with one or many people - without having to travel. It is not a replacement for all face to face meetings and depending on the content of the meeting, video conferencing may not be appropriate. At R.E.A.L. Education we use video conferencing between professionals within the organisation to:

- Improve communication
- Increase productivity
- Reduce the need for travel

Best practice guidelines for using video conferencing

Who can you video conference with?
Staff will have access to Google Meets, a video conferencing service provided to connect and

communicate with each other. The use of this service is for professional use only during work time. Video conferencing can be used by adults professionally within and outside of the R.E.A.L. Education's Google Apps suite. Video conferencing is not permitted for use with learners without prior consent from the Head of Schools as outlined above.

Video conferencing for teaching and learning

- The use of videoconferencing with learners will be planned and confirmed by the Head of Schools or Learning Manager.
- The use of Google Hangouts with multiple learners is not permitted without the explicit authority of the Head of Schools.
- The Head of Schools or Learning Manager will decide if a specific activity risk assessment is necessary.
- Staff should remind the other party about acceptable behaviour/terms of use.
- Staff will never leave children unattended when a video conference is in progress.

Respecting privacy and confidentiality

- Staff should consider the content of the meeting and the surroundings of all participants e.g. discussing sensitive personal information when unaware who else is in a participants room.
- Please remember that you do not always know where other people are (in a staff room / public space) and who can hear - professionalism should be maintained when talking about learners.
- Look behind you in the space you intend to video conference, is there anything on the wall behind that could be confidential? If so, please remove or change the location of the conference. With high definition cameras, even small text on a note can be read very easily by other people in the video conference.
- It may be appropriate to add a sign to the room you are video conferencing in that says 'Video conference in progress, please do not disturb'. Or a note on the back of your laptop with a similar message.
- When talking about learners you should not be in a public place, or a busy area (either inside the school or outside of the school). An empty room is best, as you can control and manage who can hear your conversation.

Locations to video conference from

Currently, video conferencing is allowed from all R.E.A.L. Education sites. Video conferencing is not allowed from your home or public environment without prior authorisation from the Head of Schools.

Consider the conversations going on around you, make sure that people that enter the space you are in, know that you are on a Video Conference. You can mute yourself in the video conference, alert the people talking close to you, then unmute yourself.

Video conferencing features

Whilst you can take photos in the meeting through video conferencing features, it is not appropriate to do so without the full consent of the other attendees and a rationale of the reason to do this.

The chat feature can be very useful in providing additional resources and web links for the video conference. The chat feature is a professional space, the chat is saved and stored for future reference. Under no circumstances should the feature be used to share any information about a learner or any information deemed sensitive or confidential. There is no facility to block, stop or manage access to the chat - therefore learners are able to send images, text and resources to all staff on the video conference. In Google Meet the chat can be turned off if you are the video conference creator.

If you intend to use screen share, prepare your digital workspace. Check your desktop and make sure it is clear of data and files/sticky notes etc... Disable notifications and pop ups, so no emails or messages appear to everyone as you share your screen.

Safeguarding
If anything is said or shown on a videoconference that raises a safeguarding concern, follow the agreed procedures as set out in the Safeguarding policy.

Withdrawal or suspension of use
The use of video conferencing is agreed and managed by the ICT Strategy group and online safety Strategy group. Video conferencing privileges can be withdrawn without notice for any reason deemed reasonable by the Head of Schools and Directors of R.E.A.L. Education.

7. How are emerging technologies managed?

The 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.

8. Guidelines for internet access

- Parents will be asked to read and understand the Online Safety rules presented in the Induction Booklet. This is their opportunity to discuss the content with their child and R.E.A.L. Education staff as required.
- 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 learner(s) in collaboration with parents/carers. It is the responsibility of the Learning Manager to tell the ICT team if a learner 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, learners will be supervised when using the internet, where Chromebooks have been authorised for use, the pupil may access only a small selection of websites. Any potentially inappropriate content is flagged through our filtering system and raised with the Senior Designated Safeguarding Lead.

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.

How will R.E.A.L. respond to any incidents of concern?

- All members of staff will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- Online safety concerns are reported via the current safeguarding and significant incident reporting processes which are overseen by the Head of Safeguarding and Standards, and the Head of Behaviour and Attitudes. Data is monitored and reported directly to the ICT Strategy Group and the R.E.A.L. Leadership Team for any ongoing action.
- The Head of Safeguarding and Standards will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- R.E.A.L. will manage online safety incidents in accordance with the Behaviour policy where appropriate. Staff to refer to ‘
- 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 online safety 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 on CPOMS either through a SIRF or Safeguarding concern in accordance with other reporting expectations.

How will Learning Platforms be managed?

A Learning Platform is a secure online space for storing data and collaborating. At R.E.A.L. we use Atmos, our Learning Platform based on 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.
- Learners/staff will be advised about acceptable conduct when using the Learning Platform, in accordance with the **Induction guide for online safety.**
- Only members of the current learner, parent/carers and staff community will have access to the Learning Platform, it is the responsibility for the People and Business Operations team to raise a ServiceDesk 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 or learners leave the school their account 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 GDPR 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 Head of Schools or Learning Manager before reinstatement.
e) A learners' parent/carer may be informed.

Learners Use of Personal Devices and mobile phones

- The R.E.A.L. Education Learner Mobile Phone policy documents the expectations around use for learners.

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 learner 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 learners 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. If a member of staff breaches this policy then disciplinary action may be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- Communication platforms will be used to raise the awareness and importance of safe and responsible internet use amongst learners.
- It is the responsibility to ensure that online safety 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 online safety policy will be formally provided and discussed with all members of staff at induction.
- **To protect all staff and learners**, the school will implement an Acceptable Use Policy for staff through the induction process and within the Student Induction Booklet.
- 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. An online safety course is provided for staff to access and updated annually.
- The online safety 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 learners.

- 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 online safety and share best practice and resources.

How will parents' support be enlisted?

- Parent's/carer's attention will be drawn to the **Learner Induction Booklet.**
- A partnership approach to online safety 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 online safety at other attended events e.g. parent evenings.
- Parents/carers will be encouraged to read the school Acceptable Use Policy for learners and discuss its implications with their children.

How will pupils be supported to stay safe

We have implemented a Digital Defense course for all students. This enables the students to review the key elements of online safety in an accessible way. The course is managed by tutors and learners are provided with a certificate on completion.

Review

This policy will be reviewed annually as the nature of online safety is rapidly changing.

How to respond

Practical guidance for dealing with online safety issues can be found on the Engineroom Online Safety page.

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 online safety 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 online safety 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.
Version 8	4.3.20 Updated and expanded section on Video Conferencing
Version 9	5.3.20 Data protection policy amended to show wording GDPR 2018. Removal of Freedom of Information request service as this is not required for non-public bodies.
Version 10	25.8.20 Changed online safety to Online Safety in response to Government guidelines. Updated to re-inforce Digital Creative self management of filtering. Updated to reinforce Hangouts being unsuitable for more than one student. Updated to reinforce the policy around internet blocking/unblocking.
Version 11	7.9.20 Added section on supporting the victim of cyberbullying.

	Agreed changes and suggestions made by Safeguarding Lead and DSL for online safety.
Version 12	24.11.21 Reviewed by Craig Wilkie. Minor changes to Google Hangouts > Google Meets to reflect the name change of video conferencing. Updated information about the chat feature as this can now be turned off by teachers who set up a video conference. Highlighted Use of Personal devices/phones chapter and suggest this is reduced and reader is sign posted to mobile phone policy that Adrian has drafted.
Version 13	12.7.22