Real Life Learning Academy Trust

E-Safety Policy

The E-Safety Policy has been read and approved by staff and Directors

Signed:

To be reviewed : March 2020

Dan Broughton

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning and therefore should be integrated within a rich, broad and balanced curriculum. In addition to this, children and young people have an entitlement to safe internet access at all times and must develop an awareness for safe internet practices and how to report any issues that they may have.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-Safety policy should help to ensure safe and appropriate use of the internet, social media and computing equipment. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The changing face of information technologies and the ever increasing pupil/student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. The school has a duty to ensure that the E-Safety policy is regularly updated in order to keep abreast of these changes.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate all risks completely. It is therefore essential, through good educational provision and best practice procedures to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT equipment and systems, both on and off the school site.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. Within Part 2 of the Education Act 2011 there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. These particular changes deal with the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices. Authorised staff have the right to search for electronic devices where they reasonably suspect that the data or files on the device in question has been, or could be used to cause harm, to disrupt teaching or break the school rules.

The schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and where known, will inform parents / carers of incidents of inappropriate E-Safety behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school

Directors:

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Directors' Board has taken on the role of E-Safety Governor .The role of the E-Safety Governor will include:

- regular meetings with the E-Safety lead
- regular monitoring of E-Safety incident logs
- reporting to the Directors

Headteacher and Senior Leaders:

- The Executive Headteacher/Head of School is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety subject lead.
- The Executive Headteacher / Head of School is responsible for ensuring that the E-Safety subject lead and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- The Executive Headteacher / Head of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Leadership Team will receive regular monitoring reports from the E-Safety subject lead.
- The Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

Computing Subject Leader :

- leads the E-Safety curriculum
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- meets regularly with Safeguarding Director to discuss current issues, review incident logs
- attends relevant meetings

- reports regularly to the Leadership Team

Technical staff:

The ICT Service provider is responsible for ensuring:

- that the schools' ICT infrastructure is secure and is not open to misuse or malicious attack
- that the schools meet the E-Safety Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that they keep up to date with the E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety subject leader / Executive Headteacher / Head of School / Class teacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff :

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Subject Leader or Leadership Team for investigation / action / sanction
- digital communications with pupils, email, Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school E-Safety and acceptable use policy
- and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead :

The designated safeguarding lead is trained in E-Safety issues and is aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school ICT systems in accordance with the E-Safety guidelines that are included in pupil Communication Books and the Internet Rules displayed in school
- have a good understanding of research skills as taught within the school curriculum
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers :

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE /

Community Users:

Community Users who access school ICT systems / website / VLE as part of the Extended School provision must be made aware of the E Safety and Acceptable Use Policy in place in school.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned E-Safety programme should be provided as part of the entire curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies both on and off the school site.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The schools will therefore seek to provide information and awareness to parents and carers through

- Letters, newsletters, web site, VLE
- Parents evenings

Education & Training – Staff

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The E-Safety subject lead will provide advice / guidance / training as required to individuals as required

Training – Directors

Directors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / E-Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association
- Participation in school training / information sessions for staff or parents

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) will also be available to the Leadership Team and kept in a secure place
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The schools maintain and support the managed filtering service provided by the LA

- The schools use appropriate internet filtering which will be tailored to the needs of the individual users.
- An appropriate system is in place for users to report any actual / potential E-Safety incident to the E-Safety Lead / Leadership Team
- The schools' infrastructure and individual workstations are protected with up to date virus software.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The schools will inform and educate users about these risks (in particular the risks attached to publishing their own images on social network sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the schools into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- As a 'data rich' environment, the school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data may be stored electronically. However, access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system. In addition to this, ALL staff will use strong passwords which will be changed regularly.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- When personal information is stored on any portable computer system, USB stick or any other removable media, the data **MUST** be encrypted and password protected.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will appoint a Data Protection Officer to ensure these safeguards (and others from the Data Protection Policy) are in place and adhered to by all staff.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults	**Pupils**

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	X							x
Taking photos on mobile phones				x				x
Use of hand held devices		x				x		
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of chat rooms / facilities				x				x
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of educational social networking sites (specifically EDMODO.com)	X				x			
Use of blogs		x				x		

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions The school policy restricts certain internet usage as follows:		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					x
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					x
	adult material that potentially breaches the Obscene Publications Act in the UK					x
	criminally racist material in UK					x
	Pornography				x	
	promotion of any kind of discrimination				x	
	promotion of racial or religious hatred				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					x	
Creating or propagating computer viruses or other harmful files					x	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					x	

On-line gaming (educational)		x			
On-line gaming (non educational)				x	
On-line gambling				x	
On-line shopping / commerce			X		
File sharing		x			
Use of social networking sites				x	
Use of video broadcasting eg Youtube		x			

Responding to incidents of misuse

It is hoped that all members of the school communities will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity such as child sexual abuse images; adult material which potentially breaches the Obscene Publications Act; criminally racist material or other criminal conduct, activity or materials, then the incident will be referred to the relevant authorities and the LA.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Pupils	Actions / Sanctions								
Incidents:	Refer to class teacher / tutor	Refer to member of SLT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be			x	x			x		

considered illegal									
Unauthorised use of non-educational sites during lessons	x	x							
Unauthorised use of mobile phone / digital camera / other handheld device		x				x			
Unauthorised use of social networking / instant messaging / personal email		x						x	
Unauthorised downloading or uploading of files			x						
Allowing others to access school network by sharing username and passwords		x			X	x	x		
Attempting to access or accessing the school network, using another student's / pupil's account		x				x	x		
Attempting to access or accessing the school network, using the account of a member of staff			x			x			
Corrupting or destroying the data of other users		x				x			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x			x			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident						x		x	
Deliberately accessing or trying to access offensive or pornographic material		x	x			x			

Staff	Actions / Sanctions							
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	x	x				x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X				x		
Unauthorised downloading or uploading of files		X				x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			x			x
Careless use of personal data		X						x
Deliberate actions to breach data protection or network security rules		X			x	x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			x	x		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	x			x		x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	x					x
Actions which could compromise the staff member's professional standing		X	x					x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	x					x
Accidentally accessing offensive or pornographic material and failing to report the incident		X			x	x		
Deliberately accessing or trying to access offensive or pornographic material		X	x		x			x