E.4 – E-Safety Guidance Policy

Policy Number	E. 4	**Review Cycle**	**3 year**	**Reviewer**
Date Created	21/08/2017	**Review Date(s)**	21/08/2020	CEO
Original Author	Operations Lead/ CEO		21/08/2023	
			21/08/2026	
			21/08/2029	
			21/08/2032	

1.1 APTCOO recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of the commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote learner achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable learners to gain access to a wide span of knowledge in a way that ensures their safety and security.

1.3 APTCOO holds steadfastly to the ethos that there should be an equitable learning experience for all learners using technology. We recognise that technology can allow learners increased access to the curriculum and other aspects related to learning.

1.4 APTCOO is committed to ensuring that all its learners will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their families, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

1.5 The nominated senior person for the implementation of the school's E-safety policy is the Headteacher.

2 Scope of policy

2.1 The policy applies to:

- All learners
- All teaching and support staff, trustees and volunteers

2.2 APTCOO will ensure that the following elements are in place as part of its safeguarding responsibilities to learners:

- A range of policies including acceptable use of policies that are frequently reviewed and updated
- Adequate training for staff and volunteers
- Adequate supervision of learners when using the internet and digital technologies

- Education that is aimed at ensuring safe use of the internet and digital technologies
- A reporting procedure for abuse and misuse.

3 Policies and Procedures

APTCOO understands that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist at APTCOO are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

3.1.1 APTCOO will seek to ensure that internet, mobile, and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

3.1.2 APTCOO expects all staff and learners to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below.

Users shall not:
Visit internet sites, make, post, download, upload or pass on, material remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting acts of violence
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues.

3.1.3 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually proactive)
- Adult material that potentially breached the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

3.1.4 In addition, users may not:

- Use the broadband providers facilities for running a private business;
- Enter into any personal transaction that involves the school or associated partners in any way
- Visit sites that might be defamatory or incur liability on the part of the school or associated partners or adversely impact on the image of the school or associated partners
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: Financial information, personal information, database and the information contained therein, computer/network access codes, and business relationships
- Internally interfere with the normal operation of the internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the internet
- Use the internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate
- Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe
- Assist with unauthorised access to facilities or services
- Undertake activities with any of the following characteristics:

    - Corrupting or destroying other users' data
    - Violating the privacy of other users
    - Continuing to use an item of networking software or hardware after request that use cease because it is causing disruption to the correct functioning of the network
    - Other misuse of the network, such as introduction of viruses
    - Use of mobile technologies (e.g. 4G, 3G or mobile internet services) in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

The following outlines what to do if a child or adult receives an abusive message or accidentally accesses a website that contains abusive material:

The abusive material should be stored, screenshot if possible and a copy sent to the Headteacher or CEO of APTCOO. The address (e.g. URL or email) linked to the abuse should also be recorded. However, the screen displaying the abusive material should be hidden from view and/or closed down as soon as possible to avoid further offence. The incident should be documented using the e-safety incident reporting form (**Appendix 1**) and our usual incident reporting procedures adopted thereafter.

4 Education and Training

4.1 APTCOO recognises that the internet and other digital technologies can transform learning; help improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

4.2 As part of achieving this, we want to create an accessible system, with information and services online, which support personalised learning and choice.

4.3 APTCOO will:

- Enable all learners to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum and appropriate to their age or individual learning levels.
- Educate school staff so that they are equipped to support learners in gaining positive experiences when online and can help learners develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of E-safety for their children and provide them with relevant information on the policies and procedures that govern the use of internet and digital technologies within APTCOO.

5 Infrastructure and Technology

5.1 Partnership working

5.1.1 APTCOO recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the network and broadband supplier. As part of our commitment to partnership working, we fully support and will continue to work with our providers to ensure that learner and staff usage of the internet and digital technologies is safe.

5.1.2 APTCOO will, as part of its wider safeguarding responsibilities, seek to ensure that partnership organisations, when working on our site, take an approach to their activities that see the welfare of the child as paramount.

6 Standards and Inspection

APTCOO recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks of learners are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of internet and other digital goes beyond the personal use of the internet and electronic mail a learner or member of staff may have, the school recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside (Educational and Inspections Act 2006, Section 89 (5)).

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and learners, APTCOO will audit the use of the internet and electronic mail in order to ensure compliance with this policy. The school will also work with its internet service provider to further ensure compliance.

6.1.3 Another aspect of monitoring, which our school will employ, is the use of mobile technologies by learners, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our learners, and where necessary, support individual learners where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 APTCOO has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the school to manage such situations in, and with confidence.

6.2.2 Where there is inappropriate or illegal use of the internet and digital technologies, the following sanctions will be applied:

<u>Child/young person</u>

- Breaches of the guidelines in this policy could ultimately result in the use of internet and digital technologies being withdrawn.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal internet use or child protection concerns.

Adult (staff and volunteers)

- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to the Headteacher so this can be taken into account for monitoring purposes.

7 Working in Partnership with Parents and Carers

7.1 APTCOO are committed to working in partnership with parents and carers and understand the key role they play in the E- safety of their children, through promoting E-safety at home and elsewhere.

7.2 APTCOO is committed to working in partnership with parents and carers who may have concerns about the use of internet, email and other digital technologies in school. In such circumstances staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

E-safety Incident/Concern Form – **Appendix 1**

Please complete as soon as possible and return to the designated person:

Headteacher or Designated Safeguarding Person: …………………………………

Name of child:		**Age of Child:**	
Date/ time/ place (home or school) of concern:			
Nature of concern/incident:			
Evidence (e.g. text, email, print out or screenshots) is the evidence still available?			
Reported by: Designation			
Other witnesses: Learners Staff/Adults			
Reported to (please name)			
Witness signature:			
Designated Safeguarding Person signature:			
Action (to be completed by designated person			
Outcome (to be completed by designated person)			

Appendix 2

Policy/ procedure for: E-Safety Guidance Policy

RECORD OF CHANGES

DATE	AUTHOR	PROCEDURE	DETAILS OF CHANGE

Appendix 3

EMPLOYEE RECORD OF HAVING READ THE POLICY

Title of Policy: E-Safety Guidance Policy

I have read and understand the principles contained in the named policy.

PRINT FULL NAME	SIGNATURE	DATE