Online Safety & Acceptable Use Policy

Introduction

1.0 This policy will be reviewed annually or at the point of any legislative or formal guidance changes and/or updates. APTCOO will also undertake a review following any related incidents

1.1 APTCOO recognises that the internet and other digital technologies provide vast opportunities for everyone to learn in engaging and innovative ways, and often making the learning experience more accessible to young people and vulnerable adults with SEND.

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 is committed to ensuring that all its learners will be able to use existing and emerging technologies safely. We are also committed to ensuring that all those who work with children, young people and vulnerable adults (*hereafter referred to as CYP/VA*), as well as their families, are educated as to the dangers that exist. This will enable everyone to take an active part in being vigilant, safeguarding both others and themselves.

1.4 While APTCOO encourages creativity and expression through using digital systems, we recognise there are responsibilities that users must exercise when using these systems.

1.5 This policy applies to:

- All learners, including post-16 students
- All teaching and support staff
- Trustees and volunteers
- Anyone whose role is mixed or is external and using APTCOO systems.

1.6 The nominated senior person for the implementation of this policy and ensuring people know their rights and responsibilities is the Headteacher.

2. Policy Scope

Everyone who works at APTCOO is responsible for ensuring both that members of the APTCOO community can learn and work safely and safeguarding the security of its IT systems. As such, all employees must ensure they always adhere to the guidelines in this policy. Should any employee be unclear on the policy or how it impacts their role they should speak to their line manager.

3. Definitions

Users: everyone who has access to any of APTCOO's IT systems. This includes:

* Permanent employees
* Temporary employees
* Volunteers
* Young people on supported employment
* Contractors
* Agencies
* Consultants
* Suppliers
* Learners and families (including post 16 and vulnerable adults)
* Customers and business partners.

Systems**:** all IT equipment that connects to the organisational network or accesses organisational applications. This includes, but is not limited to:

* Desktop computers & laptops
* Smartphones & tablets
* Printers
* Data and voice networks
* Networked devices
* All system licensed and/or utilised software
* All electronically stored data
* Portable data storage devices
* Third party networking services
* Telephone handsets
* Video conferencing systems

3.1. APTCOO will ensure that the following elements are in place as part of its safeguarding responsibilities:

- A range of policies, including this one, 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 promotes the safe use of the internet and digital technologies
- A reporting procedure for abuse and misuse.
- Consistent vigilance and monitoring of internet, mobile and digital technologies.

2 Policies and Procedures

APTCOO understands that effective policies and procedures are the backbone to developing a whole-school approach to online safety. The policies that exist at APTCOO are aimed at providing a balance between exploring the educational potential of new technologies and ensuring vigilance and effective monitoring to provide safeguards to learners. They will be reviewed at regular intervals.

This policy includes aspects of these additional policies:

- Data Protection
- Safeguarding
- Code of Conduct
- Behaviour for Learning

This policy also incorporates the following legislation:

- Copyright, Designs and Patents Act 1988
- Malicious Communication Act 1988
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Trade Marks Act 1994
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Communications Act 2003
- Defamation Act 2013
- General Data Protection Act 2018

APTCOO's policy and practice also incorporate best practice guidance from the London Grid for Learning (LGfL).

3. ONLINE SAFETY

3.1 The online world of learning, engagement and inspiration is also an online world of risk and potential safeguarding issues. These cannot be eliminated from our lives, but through personal awareness, robust policies and procedures, and an open culture, APTCOO will minimise these risks within the school setting.

3.2 To achieve this APTCOO will:

- Enable all learners to develop and exercise the skills of critical awareness, digital literacy, and good online citizenship as part of the school curriculum, appropriate to their age or individual learning levels.
- The teaching of online safety will be included in the provision for all CYP/VA at APTCOO. This provision includes key messages that are age/ability appropriate, such as keeping personal information safe and secure, how to deal appropriately with cyberbullying, and knowing that there are trusted people they can tell if they encounter inappropriate content/contact online.

- Educate 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 online safety for their CYP/VA and provide them with relevant information on the policies and procedures that govern the use of internet and digital technologies within APTCOO.

- Maintain an open and honest culture where concerns and challenges can be raised, discussed, and resolved through the appropriate channels, either before they fully emerge or at the first possible opportunity.

4. Partnership working

Parents and carers

4.1 APTCOO is committed to working in partnership with parents and carers and understand the key role they play in the online safety of their CYP/VA, through promoting online safety at home and elsewhere.

4.2 APTCOO will communicate with parents and carers who may have concerns about the use of digital technologies in school. In such circumstances staff will meet with parents

and carers to discuss their concerns and, if the parental figures wish, agree upon a series of alternatives that will allow their CYP/VA to fully access the curriculum, whilst remaining safe.

5. Other organisations

5.1 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 and secure.

5.2 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, young person, or vulnerable adult as paramount.

6. Access

6.1 If inappropriate material is accessed, users are required to immediately report this to the Headteacher, SENCO and/or DSL so this can be considered for monitoring purposes. Each situation will be judged on a case-by-case basis.

6.2 If a child or adult receives an abusive message or accidentally accesses a website that contains abusive material, said material should be stored, recorded in a screenshot if possible and a copy sent to the Headteacher, SENCO or other Designated Safeguarding Lead. The abusive content may be either generalised or specifically about the individual who received the message.

6.3 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.

6.4 The incident should be documented using the online safety incident reporting form outlined in **Appendix 1** and our usual incident reporting procedures adopted thereafter. This is also for monitoring purposes.
The details will only be recorded in full within the online safety incident form in Appendix 1.
Where the incident involves nudity or other sexual imagery involving children under the age of 18, staff must never download, share or deliberately view the images themselves, nor must they ask the child to download or share the images. If accidentally viewed, this must be reported to the DSL.

The images themselves must not be deleted, nor should staff ask the child to disclose information about the incident – this is the responsibility of the DSL. If accidentally viewed, this must be reported to the DSL.

7. PREVENT DUTY

7.1 Under the Counter-Terrorism and Security Act 2015, APTCOO has a statutory duty to assist the prevention of people being drawn into terrorist activity. This is known as the Prevent Duty.

7.2 APTCOO members must not create, download, store or transmit/publish any material which is either unlawful, or indecent, offensive, defamatory, threatening, discriminatory or extremist.

7.3 The Prevent Duty is at the heart of safeguarding and all staff who discover such content must, in the first instance, report to their line manager and/or the Designated Safeguarding Lead.

7.4. APTCOO has a dedicated PREVENT DSL **– Joe Lloyd**

8. ACCEPTABLE USE

8.1 APTCOO expects all staff and learners to use the internet, mobile and digital technologies responsibly according to the conditions below. It is important that staff promote best practice and be a good role model for young people in their use of online media and resources.

Users shall not:

Visit internet sites, make, post, download, upload or pass on remarks, proposals or comments that contain or relate to:

- Indecent 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
- Promotes online sexual abuse
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting acts of violence or weapon-making
- Promoting illegal acts
- Any other information or activity which may be offensive to peers or colleagues, or which breaches the code of conduct and/or UK law.

8.2 In addition, users may not use, create, or transmit any of the following:

- Using the network to run a private business.
- Enter any personal transaction that involves the school or associated partners
- Visit sites that might be defamatory or incur liability on the part of the school or associated partners, or adversely impact other image of the school or associated partners. They must also not create or transmit any material involving the above.
- Upload, download, store or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties without appropriate licensing or authorisation.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - Financial information or personal information
    - The organisational database and its information
    - Computer/network passwords or other access codes.
    - Business relationships
- Intentionally interfere with the normal operation of the network, including spreading computer viruses and sustained high volume network traffic, such as:
    - Sending or receiving of large files
    - Sending and receiving of large numbers of small files
    - Any other activity that causes network congestion or that substantially hinders others in using the internet.
- Circumventing APTCOO's IT security systems and protocols.
- The use of any APTCOO networks, facilities or devices, or activity directed at APTCOO members, which is intended to embarrass, frighten, or harass an individual. This is cyber-bullying and will not be tolerated in any capacity.
- 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 users or organisations, unless the material is embedded within, or is otherwise part

of, a service to which the member of the user organisation has chosen to subscribe.

- Aid and abet others in the unauthorised access and use of organisational networks and resources.

9. Bring Your Own Device(s) (BYOD)

9.1 The policy also covers devices that are not owned by the organisation and are owned by employees who use them for work purposes. These are known as bring-your-own device (BYOD). APTCOO recognises that BYODs are an integral part of the organisation's ability to work efficiently and permit their use. However, users of BYODs must agree to certain criteria before they can be used to access APTCOO's digital systems. This is to minimize the threat of data loss or any other system compromise and will be implemented for all users of APTCOO's systems.

10. Personal use

10.1 APTCOO's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be detrimental to users' own or their colleague's productivity and nor should it result in any direct costs being borne by APTCOO other than for trivial amounts. Employees are trusted to be fair and sensible when deciding what is an acceptable level of personal use.

10.2 Users must always guard against the risk of malware being imported into APTCOO's systems and must report any actual or suspected malware infection immediately.

11, Unacceptable Use

11.1 The activities below are provided as examples of unacceptable use, if done deliberately, both on APTCOO network and mobile networks:

- All activities which have a negative impact on the success of APTCOO.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business (e.g., streaming media which does not facilitate or assist a work or education environment, playing video games and using social media including Facebook and Twitter for personal use).
- The creation and/or transmission of material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety.
- Any anti-social or unacceptable use of the ICT system, including passing on chain messages, spam or other unsolicited advertising for personal gain, or hoax virus

warnings.

- Wasting staff time or networked resources or disrupting others' work.
- Corrupting or destroying other users' data

- Violating the privacy of other users
- Using the network resources or Internet in a way that denies service to other users (e.g., deliberately overloading access links or switches)
- Other misuse of digital resources which include the introduction of malware into the system.

- Where APTCOO digital resources are being used to access another network, any abuse of said network's acceptable use policy will be regarded as unacceptable use by APTCOO itself.

- 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

11.2 Should an employee need to contravene these guidelines in order to perform their role, they should consult and obtain approval from their manager before proceeding.

12 Monitoring

12.1 APTCOO can monitor the use of its IT systems and the data contained within. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of their access history. APTCOO reserves the right to regularly audit networks and systems to ensure compliance with this policy.

12.2 In line with the Education and Inspections Act 2006 (Section 89 (5)), we reserve the right to consider public postings by its staff on social media platforms when considering conduct and behaviour.

12.3 The school will also work with its internet service provider to further ensure compliance.

12.4 Another aspect of monitoring employed by APTCOO 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).**

12.5 We will also ensure that school staff understand the need to be vigilant and to monitor our learners, and where necessary, support individual learners where they have been deliberately or inadvertently been subject to harm.

13. Sanctions and enforcement

13.1 APTCOO has been careful to develop 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.

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

- Breaches of the guidelines in this policy could ultimately result in the use of internet and digital technologies being withdrawn, in the case of children, young people or vulnerable adults. In the case of staff and volunteers, they may be subject to disciplinary process.
- 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.

Appendix 1

Online 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, young person or vulnerable adult:		**Age of CYP/VA:**	
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: Online Safety & Acceptable Use Policy

RECORD OF CHANGES

DATE	AUTHOR	DETAILS OF CHANGE
March 2022	Compliance Lead	V1 'Learners' and 'Service Users' added to paragraph 2 – Definitions under 'Users'. Updated references to online sexual abuse in line with amendments made to the Ofsted inspection handbook Feb 2022.
October 2022	Mike Holmes	V2 Review and update in line with best practice guidance

Appendix 3

EMPLOYEE RECORD OF HAVING READ THE POLICY

Title of Policy: Online Safety & Acceptable Use Policy

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

PRINT FULL NAME	SIGNATURE	DATE