Online Safety Policy

Version Number:
- 4

Applies To:
- APTCOO Charity Services
- APTCOO Independent Special School
- APTCOO Short Breaks
- APTCOO Out of School Activities

Associated Documents:
- Safeguarding and Child Protection policy
- Bullying policy
- Relational policy
- Staff Code of Conduct/Disciplinary procedures
- Data Protection policy and privacy notices
- Concerns, Complaints, Compliments policy
- Information Security & Acceptable Use policy

Related Regulations:
- Keeping Children Safe in Education 2024
- The Equality Act 2010
- UK council for internet safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Education and Inspections Act 2006
- Gov.UK Protecting Children from Radicalisation (The PREVENT Duty)
- The Charity Commission for England and Wales

Review Frequency:
- Annually

Date of Implementation:
- Autumn 2024

Review Date:
- Autumn 2025

Chief Executive Officer (CEO) Date 5/12/24	Chair of Board of Trustees /Governing Board Date 5/12/24

Aims and Scope

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.

APTCOO aims to:

- Have robust processes in place to ensure the online safety of learners, young people, staff, families, volunteers and governors.
- Identify and support groups of young people that potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the entire APTCOO community in its use of technology, including mobile and smart technology (hereafter referred to as 'mobile devices').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The four key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content –** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact –** being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children/young people with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct –** personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes, semi-nudes, and/or pornography), sharing other explicit images, and online bullying.
- **Commerce –** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.1 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.

Should any employee be unclear on the policy or how it impacts their role they should speak to their line manager.

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

1.3 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,

2 Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying
- Relationships and sex education
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from radicalisation (The PREVENT Duty).

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, and the Equality Act 2010.

Roles and responsibilities

The Board

The Board of Trustees/Governing Board, hereafter referred to as 'the Board', has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Board will ensure all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles and responsibilities around filtering and monitoring within their work environment.

The Board will also make sure all staff receive regular online safety updates (via email, e-bulletins, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Board should ensure that children are taught how to keep themselves and others safe, including keeping safe online.

The Board must ensure APTCOO has appropriate and robust filtering and monitoring systems in place on work and education devices and networks and will regularly review their effectiveness. The Board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support APTCOO in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understood this policy
- Agree and adhere to the terms on acceptable use of APTCOO's IT systems and the internet (see appendix)
- Ensure that online safety is a running and interrelated theme while devising and implementing a whole-organisation approach to safeguarding and related policies and/or procedures.
- Ensure that learning about safeguarding and online safety is thoroughly adapted for SEND needs, victims of abuse, and especially vulnerable children.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout APTCOO.

The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead, as well as their deputies, are set out in our Safeguarding and Child Protection policy, as well as relevant job descriptions.

The Headteacher, also being the primary DSL, takes lead responsibility for online safety at APTCOO. This includes the following areas:

- Working with the Compliance Lead, IT & Systems Coordinator, and the Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.

- Having a working understanding of the filtering and monitoring systems and processes in place on APTCOO devices and networks.

- Working with the IT & Systems Coordinator to be assured that the appropriate systems and processes are in place.

- Working with the IT & Systems Coordinator and other staff, as necessary, to address any online safety issues or incidents.

- Managing all online safety issues and incidents in line with APTCOO's Safeguarding and Child Protection policy.

- Ensuring that any online safety incidents are logged (see appendix) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with APTCOO's Relational policy.

- Liaising with other agencies and/or external services if necessary.

- Providing regular reports on online safety in APTCOO to the headteacher or Board.

- Undertaking annual risk assessments that consider and reflect the risks children face.

- Providing regular safeguarding and child protection updates, including online safety, to all staff at least annually to provide them with continuing relevant skills and knowledge to safeguard effectively.

The IT and Systems Coordinator

The IT and Systems Coordinator is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on APTCOO devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure children are kept safe from potentially harmful and inappropriate content and contact online while at APTCOO, including terrorist and extremist material.
- Ensuring that APTCOO'S IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting regular full security checks and monitoring APTCOO's IT systems on a consistent, weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with APTCOO's behaviour policy.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of APTCOO's IT systems and the internet (see appendix) and ensuring that young people follow APTCOO's terms on acceptable use.
- Knowing the headteacher/lead DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by following the correct procedure.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix) and dealt with appropriately in line with this policy.
  Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes, which will be confirmed and agreed by the headteacher
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with APTCOO's Relational policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of APTCOO's IT systems and internet.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent/carer resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use APTCOO's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating learners about online safety

Learners will be taught about online safety as part of the curriculum. Learners will be taught in a personalised and individual curriculum about a wide range of risks and safety measures.

The safe use of social media and the internet will be a central part of this curriculum and will be covered in both measurable ways and ad hoc conversations, with the details to be recorded.

Educating parents/carers about online safety

APTCOO will raise parents/carers' awareness of online safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during meetings and conversations with parents/carers.

APTCOO will let parents/carers know what systems the school uses to filter and monitor online use.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/ DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyberbullying

Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (for more information, see the Relational policy).

Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that young people understand what it is and what to do if they become aware of it happening to them or others. We will ensure that young people know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyberbullying with learners, explaining the reasons why it occurs, the form it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support young people, as part of their annual Safeguarding and Child Protection and PREVENT awareness training. Definitions of cyberbullying and its impact are also outlined in the annual Online Safety training course that all delivery staff access.

APTCOO will also send information on cyberbullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyberbullying, APTCOO will follow the processes set out in APTCOO's Relational policy. Where illegal, inappropriate, or harmful material has been spread among learners, APTCOO will use all reasonable endeavours to ensure the incident is contained.

If the DSL has reasonable grounds to suspect that possessing certain material is illegal, they will report the incident and provide the relevant material to the police as soon as is reasonably practical. They will also work with external services if it is deemed necessary to do so.

Nudes and semi-nudes

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they must:

- **Not** view the image, nor download or share the image, or ask the child to download or share the images. If accidentally viewed, this **must** be reported to the DSL.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation, and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any search of a young person will be carried out in line with the above guidance.

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school complaints procedure.

Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now both widespread and easy to access. Staff, young people and parents/carers may be familiar with generative chatbots such as ChatGPT, DALL·E, and Midjourney.

APTCOO recognizes that AI has many uses to help young people learn but may also have the potential to be used to bully others. One example is in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

APTCOO will treat **any** use of AI to bully young people in line with our Bullying and Relational policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools, particularly ones involving image generation, are being used within APTCOO.

Acceptable use of the internet in school

All learners, parents/carers, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of APTCOO's IT systems and the internet. Visitors will be expected to read and agree to APTCOO's terms on acceptable use if relevant.

Use of APTCOO's Internet must be for educational purposes or fulfilling the duties of an individual's role. While we accept a certain degree of personal use, this must not impact negatively on people's learning or productivity.

We will monitor the websites visited by young people, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the Acceptable Use policy, which applies to all members of the APTCOO community.

Young people using mobile devices in school

Young people are permitted to bring their personal mobile phones into school, pending acceptance of the general terms of use. Any other non-necessary electronic devices will be subject to an agreement with the Headteacher.

Staff using work devices outside APTCOO hours

All staff will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a set time period.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate APTCOO's terms of acceptable use.

Work devices must be used for work activities, though a small amount of personal use is acceptable, provided it is in line with the Information Security & Acceptable Use policy**.**

If staff have any concerns over the security of their device, they must seek advice from the IT & Systems Coordinator. More information on all of these points can be found in APTCOO's Information Security & Acceptable Use policy.

How APTCOO will respond to issues of misuse

Where a learner misuses APTCOO's IT systems or the internet, we will follow the procedures set out in this appendix as well as our Relational policy. The action taken will be dependent on the individual circumstances, nature and seriousness of the specific incident and will be proportionate.

Where a staff member misuses APTCOO's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

APTCOO will consider whether incidents that involve illegal activity or content should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure young people can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence young people to make the healthiest long-term choices and keep them safe from harm in the short term.

Both the primary DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if and when applicable.
More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

Monitoring

The DSL logs behaviour and safeguarding issues related to online safety. An incident reporting log will be available on the APTCOO Portal for internal submission and processing.

This policy will be reviewed annually by the IT & Systems Coordinator. At every review, the policy will be shared with the Board. The review will be supported by an annual risk assessment that considers and reflects the risks young people face online. This is crucial because technology, and the associated risks and harms, evolve and change rapidly.

Links with other policies

The Online Safety policy is linked to our:

- Safeguarding and Child Protection policy
- Bullying policy
- Relational policy
- Staff Code of Conduct/Disciplinary procedures
- Data Protection policy and privacy notices
- Concerns, Complaints, Compliments policy
- Information Security & Acceptable Use policy

Appendix 1

Policy/ procedure for: Online Safety 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
September 2023	Mike Holmes	V3 update – reformat of information and addition of key categories of risk
August 2024	IT & Systems Coordir	V4 update – clarification of wording and minor cosmetic changes.