
Legal and Statutory Framework

This policy is underpinned by:

- Keeping Children Safe in Education (KCSIE) (current version).
- Working Together to Safeguard Children.
- Alternative Provision Statutory Guidance.
- UK GDPR and Data Protection Act 2018.
- Children Act 1989 and 2004.
- Equality Act 2010.

This policy should be read alongside:

- Winchmore Tutors Child Protection and Safeguarding Policies.
- Winchmore Tutors Staff Code of Conduct.
- Winchmore Tutors Managing Allegations Against Staff Policy.
- Winchmore Tutors Lone Working Policy.
- Winchmore Tutors Data Protection Policy.

Online Safety

Winchmore Tutors recognises that safeguarding and promoting the welfare of children is everyone's responsibility.

Online safety forms a key part of our safeguarding arrangements. The welfare of the child remains paramount at all times.

Many pupils receiving online tuition through Winchmore Tutors may be vulnerable due to SEND, SEMH needs, school absence, Alternative Provision arrangements, trauma, adverse childhood experiences or other safeguarding concerns.

All staff must adopt a child-centred approach and ensure that online learning environments are safe, inclusive and supportive.

The internet is an amazing resource which enables children and young people to connect, communicate and be creative in a number of different ways, on a range of devices.

However, the internet is always changing, and being able to keep up to date with your children's use of technology can be a challenge.

You may sometimes feel that your children have better technical skills than you do, however children and young people still need advice and protection when it comes to managing their lives online.

Issues that your child may encounter on the internet will vary depending on their age and online activities. We have grouped potential online risks into these 4 categories.

Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When

using the internet, it's important to keep personal information safe and not share it with strangers. Discuss with your child the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

Content: age-inappropriate or unreliable content can be available to children

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need your help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Contact: children can be contacted by bullies or people who groom or seek to abuse them

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk). If your child is the victim of cyberbullying, this can also be reported online and offline. Reinforce with your child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Commercialism: young people can be unaware of hidden costs and advertising in apps, games and websites

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Encourage your children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

Alternative Provision (AP) Online Safeguarding Risks

Winchmore Tutors recognises that pupils educated through Alternative Provision may experience increased vulnerability online.

This may include:

- Increased social isolation.
- Reduced peer interaction.
- Mental health and emotional wellbeing needs.
- SEND and communication needs.
- Increased susceptibility to grooming, exploitation and radicalisation.
- Difficulties recognising online risk.
- Attendance concerns.
- Trauma-related vulnerabilities.

Risk assessments should consider these factors and appropriate safeguards should be implemented before online provision commences.

PROHIBITED COMMUNICATION METHODS

Staff must not communicate with pupils using:

- WhatsApp.
- Snapchat.
- Instagram.
- Facebook.
- TikTok.
- Discord.
- Telegram.
- Personal email accounts.
- Personal mobile phones.
- Gaming platforms.
- Any personal social networking platform.

Communication with pupils must only occur through approved Winchmore Tutors systems and authorised tuition platforms.

Staff must not:

- Accept friend requests from pupils.
- Follow pupils on social media.
- Share personal contact details.
- Use disappearing or encrypted messaging applications with pupils.
- Communicate outside agreed educational purposes.

Device Security

Any device used to deliver online tuition must:

- Be password protected.
- Use multi-factor authentication where available.
- Have updated operating systems and security patches installed.
- Use current anti-virus and anti-malware software.
- Have encrypted storage where possible.
- Automatically lock after a period of inactivity.

Staff must:

- Keep devices secure at all times.
- Prevent unauthorised access to pupil information.
- Not allow family members or other individuals access to tuition sessions.
- Store pupil information securely.
- Immediately report lost, stolen or compromised devices.

Sessions should only be delivered from appropriate professional environments where confidentiality can be maintained.

Online Teaching Expectations

Staff delivering online tuition must:

- Use only approved platforms.
- Ensure professional dress and conduct.
- Deliver sessions from an appropriate private environment.
- Use neutral and professional backgrounds.
- Maintain professional boundaries.
- Keep a record of attendance and significant incidents.

One-to-one online tuition should be risk assessed and subject to appropriate safeguarding oversight.

Any safeguarding concern arising during an online session must be reported immediately through internal safeguarding procedures.

Safeguarding Reporting Procedures

Any online safety concern must be reported immediately to the Designated Safeguarding Lead (DSL).

This includes concerns relating to:

- Grooming.
- Exploitation.
- Radicalisation.
- Cyberbullying.
- Self-harm.
- Suicidal ideation.
- Harmful sexual behaviour.
- Online abuse.
- Sharing of inappropriate images.
- Online contact from unknown adults.

Staff should never investigate concerns independently.

All concerns must be recorded using Winchmore Tutors' safeguarding reporting procedures and submitted without delay.

Designated Safeguarding Lead (DSL)

Winchmore Tutors has a Designated Safeguarding Lead (DSL) who takes lead responsibility for safeguarding and child protection across the organisation.

Designated Safeguarding Lead

Name: Craig Varney

Deputy Designated Safeguarding Lead

Name: Dan Stagg

The Winchmore Tutor's Child Protection Number is : 01372 940 808

Escalation Procedures

Where concerns involve staff conduct, professional boundaries or online interactions between adults and children, the matter must be reported immediately to the DSL.

The DSL will:

- Assess immediate risk.
- Consider whether the concern meets the harm threshold.
- Consult the LADO where appropriate.
- Follow the Managing Allegations Against Staff Policy.
- Ensure appropriate records are kept.

No member of staff should attempt to investigate allegations involving adults working with children.

Filtering & Monitoring

Pupils using the internet during lessons will be monitored at all times to ensure they are accessing suitable content. However, as tuition is not carried out on our premises the student will not be accessing the internet on a Winchmore Tutors network so any use will be subject to the premises filtering and monitoring policies.

Misinformation, Disinformation and Conspiracy theories

Misinformation (unintentional false info), disinformation (deliberate, harmful, or misleading content), and conspiracy theories (narratives blaming covert actions by powerful groups) are major, overlapping threats that fuel social division, mistrust, and harm. They spread via social media's echo chambers and are often designed to manipulate public opinion or cause harm.

Disinformation - fake or misleading stories created and shared deliberately often by a writer who might have a financial or political motive.

Misinformation - This also means fake or misleading stories, but in this case the stories may not have been deliberately created or shared with the intent to mislead.

Conspiracy theories - offer a simplified model for things that cannot be explained or easily understood. They typically involve an 'alternative' explanation for an event to those provided by governments or official international bodies, sometimes suggesting a group, individual or organisation is responsible or hiding information from the public

Fake News - is another term that is widely used that means the news is not reliable or truthful. It is also used to refute a claim, which could in fact be true!

Fake news fails to capture the complex problem of disinformation, which is often the skillful blending of 'facts' with the fabricated to create something that goes beyond anything resembling 'news'. On social media, this will involve a whole array of digital behaviour deliberately designed to mislead.

Why is it important?

- Impact of disinformation - whilst disinformation may not necessarily be illegal it can have a damaging impact on people and the wider society. Especially when its aim is to disrupt or challenge the democratic process, the integrity of elections and the values that shape public policies such as finance and health.
- Risk to mental health - disinformation and misinformation can lead to an increase in anxiety, damage to self-esteem and skewed view of the world. Conspiracy theories will encourage a sense of suspicion and potentially exaggerate tensions or make perceived threats more persuasive.
- Risks to young people - disinformation spreads more quickly on social media than verified news. Echo chambers and filter bubbles are used to promote disinformation. This can lead to stronger or more extreme viewpoints and can fuel resentment.

Echo chambers are social spaces in which the same or similar ideas, opinions and beliefs are repeated within a closed group. This can stop people from appreciating other points of view on a topic.

Filter bubbles occur online when users are suggested content based on their previous internet consumption habits, and can lead to them being separated from information that disagrees with their viewpoint.

What can I do to support young people?

Guardians/schools/staff working online with pupils during WT tutoring need to educate pupils to identify false or misleading content and protect them from manipulation.

If you have any concerns relating to a young persons use of the internet please report this to the DSL in line with our Child Protection Policy which can be found on our website by clicking [here](#).

More information can be found at <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>