



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

ASPIRIO LTD ONLINE SAFETY POLICY

POLICY

This policy applies to all members of Aspirio (including mentors, mentees, parents and carers, and community users) who have access to and are users of digital systems about Aspirio.

Created March 2025

The following review date is March 2026

SCOPE OF THE ONLINE SAFETY POLICY

Aspirio Ltd works with children and families as part of its activities. These include nurturing children's confidence and motivation through personalised coaching and mentoring. To achieve this, we offer individualised programs and use proven strategies to create a nurturing environment where each child can thrive and reach their full potential.

This Online Safety Policy outlines:

- Aspirio's commitment is to safeguard members of our community online through statutory guidance and best practices.
- Ensuring the safety and well-being of children and young people is paramount when adults, young people or children use the internet, social media or mobile devices.
- Provide staff with the overarching principles guiding our online safety approach.
- To ensure that, as an organisation, we operate by our values and within the law regarding how we use online devices.

ASPIRIO ETHOS

We believe that:

- ❖ Children and young people should never experience any form of abuse.
- ❖ Children should be allowed to use the Internet for educational and personal development purposes, but safeguards must be in place to always ensure their safety.



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

We recognise that:

- ❖ The online world offers many opportunities but presents risks and challenges.
- ❖ We must protect our organisation's children, young people, and adults from potential online harm.
- ❖ All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all forms of harm or abuse.
- ❖ Collaborating with children, young people, their parents, carers, and other agencies is essential for promoting their welfare and helping them understand how to approach online safety responsibly.

SCHEDULE FOR DEVELOPMENT, MONITORING AND REVIEW

Aspirio Ltd approved this Online Safety Policy on March 6, 2025.

Kylie Stewart, Founder and Director, will monitor the implementation of this policy. Monitoring will occur regularly, and the Online Safety Policy will be reviewed annually or more frequently if significant technological developments, online safety threats, or incidents arise.

The following review date will be March 2026.

Kylie Stewart should be informed of serious online safety incidents.

Aspirio Ltd will evaluate the effectiveness of the Online Safety Policy by maintaining logs of reported incidents, conducting internal monitoring of mentor activity when necessary, and contacting parents or guardians if any incident concerns are raised.

POLICY AND LEADERSHIP

****Responsibilities****

To ensure the online safety of Aspirio Ltd's members, everyone in the community must work together to develop safe and responsible online behaviours. This includes learning from each other and best practices and reporting inappropriate or unsafe online behaviours, concerns, or misuse as soon as they arise.

****The Founder: ****

- ❖ Has a duty of care to ensure the community's safety, including online safety, and promote a safeguarding culture.
- ❖ Should be familiar with the procedures if a serious online safety allegation is made against an employee.
- ❖ Is responsible for ensuring that all mentors effectively fulfil their responsibilities and receive appropriate training to perform their roles.



ASPIRIO

**Registered office : The Braes,
Granville Road, Bath. BA1 9BE**

****Mentors: ****

Mentors are responsible for ensuring that:

- ❖ They know current online safety issues and trends and the Aspirio Ltd Online Safety Policy and Practices.
- ❖ They understand that online safety is an essential part of safeguarding.
- ❖ They immediately report any suspected misuse or problems to the Director of Aspirio Ltd for investigation and action, following Aspirio Ltd.'s safeguarding procedures.
- ❖ All digital communications with mentees and their parents or carers are professional. Parents must approve any communication outside of scheduled sessions in advance. Mentors should be able to provide proof of such permission if requested.
- ❖ Online safety issues are integrated into all Aspirio Ltd.'s activities.
- ❖ Mentees must adhere to national safeguarding guidance and follow Aspirio Ltd.'s safeguarding policies when using live streaming or videoconferencing.
- ❖ Uphold a zero-tolerance policy against online bullying, sexual harassment, discrimination, and hatred.
- ❖ Model safe, responsible, and professional online behaviours using technology, including social media.

****Parents and Carers: ****

Parents and caregivers play a vital role in helping their children understand the importance of appropriately using online services and devices. Aspirio Ltd is committed to supporting parents and caregivers in this endeavour by:

- ❖ Publishing its Online Safety Policy on the Aspirio Ltd website.
- ❖ Obtain consent for digital images, recordings, and external contact and address any online safety concerns.
- ❖ Address parents' questions or concerns about online safety through email, messages, phone calls, or Aspirio Ltd.'s social media platforms, and guide to additional online safety resources.

Parents and caregivers are encouraged to support Aspirio Ltd by:

- ❖ Reinforcing the online safety messages shared with their children.
- ❖ Ensuring the safe use of their children's devices.
- ❖ Guiding their children in the responsible use of online accounts.



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

****Professional Standards: ****

There is an expectation that required professional standards will be applied to online safety as in other aspects of Aspirio Ltd, i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of Aspirio Ltd and its wider community.

POLICY

****Online Safety Policy****

The Department for Education (DfE) guidance, "Keeping Children Safe in Education," states that "online safety and the school or college's approach to it should be reflected in the child protection policy."

Although Aspirio Ltd is neither a school nor a college, we work closely with schools and local authorities, as well as with school-age children and young people. Therefore, our policies and protocols are aligned with those of educational bodies.

THE PURPOSE OF THIS POLICY STATEMENT

****Aspirio Ltd.'s Online Safety Policy****

Purpose: This policy sets clear expectations for the safe and responsible use of digital technologies in learning, administration, communication, and recreation.

Responsibilities: It defines the policy's responsibilities for implementing and upholding.

Regular Review: The policy is regularly reviewed in collaboration with relevant stakeholders, considering online safety incidents and emerging trends in technology and behaviour.

Guidance for Mentors: It provides guidelines for using digital technologies responsibly, ensuring their safety and that of Aspirio Ltd. while helping safeguard their mentees in the digital environment.

Support for Mentees: The policy outlines how Aspirio Ltd. will prepare and support mentees to be safe and responsible users of online technologies.

Reporting Procedures: It establishes clear procedures for identifying, reporting, responding to, and recording the misuse of digital technologies and online safety incidents.

Accessibility: The policy is published on Aspirio Ltd.'s website for easy access.



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

***ASPIRIO WILL SEEK TO KEEP CHILDREN AND YOUNG PEOPLE SAFE BY: ***

- ❖ Appoint an online safety coordinator (this may or may not be the same person as your designated child protection lead).
- ❖ Provide clear and specific guidelines to staff and volunteers on expected online behaviour, as outlined in our behaviour code for adults.
- ❖ Support and encourage young people using our service to safely use the Internet, social media, and mobile phones while showing respect for others.
- ❖ Support and encourage parents and carers to take steps to keep their children safe online.
- ❖ Develop an online safety agreement that can be used with young people and their parents or carers.
- ❖ Establish clear and robust procedures to effectively respond to inappropriate online behaviour by adults, children, or young people.
- ❖ Regularly review and update the security of our information systems.
- ❖ Ensure that usernames, logins, email accounts, and passwords are utilised effectively.
- ❖ Safeguard personal information related to adults and children involved in our organisation, ensuring it is shared only when appropriate.
- ❖ Obtain written permission before using images of children, young people, and families, and use them solely for the purpose for which consent was given.
- ❖ Provide supervision, support, and training for staff and volunteers regarding online safety.
- ❖ Examine and assess risks associated with any social media platforms and new technologies before they are used in the organisation.

***UNACCEPTABLE USE: ***

Aspirio has defined what it regards as unacceptable use below:

- ❖ Users shall not access online content (including apps, games, and sites) to make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:
 - Any illegal activity, for example:
 - Child sexual abuse imagery*
 - Child sexual abuse/exploitation/grooming
 - Terrorism
 - Encouraging or assisting suicide
 - Offences relating to sexual images, i.e., revenge and extreme pornography
 - Incitement to and threats of violence
 - Hate crime
 - Public order offences - harassment and stalking
 - Drug-related offences
 - Weapons/firearms offences
 - Fraud and financial crime, including money laundering



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

- ❖ Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):
 - Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)
 - Gaining unauthorised access to Aspirio Ltd networks, data and files using computers/devices
 - Creating or propagating computer viruses or other harmful files
 - Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)
 - Disable/Impair/Disrupt network functionality using computers/devices

***IF ONLINE ABUSE OCCURS, ASPIRIO WILL: ***

- ❖ Establish clear and robust safeguarding procedures for addressing all forms of abuse, including online abuse.
- ❖ Provide support and training for all staff and volunteers on how to handle various types of abuse, such as bullying (including cyberbullying), emotional abuse, sexting, sexual abuse, and sexual exploitation.
- ❖ Ensure that our response considers the needs of the person experiencing abuse, any bystanders, and our organisation.
- ❖ Regularly review the plan developed to address online abuse to ensure that any issues are effectively resolved in the long term.

This Online Safety Policy applies to all members of the Aspirio community, including mentors, mentees, parents, carers and guardians who have access to digital systems linked to Aspirio Ltd. It has been drawn up based on legislation, policy, and guidance that seek to protect children in England, Northern Ireland, Scotland, and Wales.

Aspirio will address such incidents within this policy and associated behaviour and will, where known, inform parents/carers of inappropriate online safety behaviour.

The Aspirio Founder and Director developed this online safety policy with similar policies. It is important to note that, in general terms, an illegal action, if committed offline, is unlawful if committed online.



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

ONLINE SAFETY EDUCATION FOR MENTEES

While regulations and technical solutions are essential, balancing them with educating learners on responsible online behaviour is crucial. Therefore, educating learners about online safety is critical to Aspirio Ltd.'s online safety program. Learners need assistance and support to recognise and avoid online safety risks and develop resilience.

Online safety should be emphasised in every Aspirio Ltd session, with mentors reinforcing online safety as part of their mentee interactions. This is achieved in the following ways:

- ❖ Tailoring online safety discussions during sessions according to age and ability.
- ❖ Assess mentees' needs and progress regarding online use and safety throughout the sessions.
- ❖ Mentors are positive role models for using digital technologies, the internet, and devices.

FAMILIES

Some parents and caregivers may have a limited understanding of online safety risks and issues, yet they play a crucial role in educating their children and monitoring their online behaviours. Often, parents underestimate how children and young people encounter potentially harmful and inappropriate material on the internet and may feel uncertain about how to respond.

Aspirio Ltd aims to provide information and raise awareness for parents and caregivers through the following initiatives:

- ❖ Communicate with parents on safety issues via Aspirio Ltd.'s social media platforms.
- ❖ Offering online safety advice on Aspirio Ltd.'s website, referencing relevant resources and publications.
- ❖ Encouraging mentees to share the online safety messages they learn during sessions with their parents.
- ❖ Allowing mentors to advise parents or guardians when needed or upon request.

TECHNOLOGY

Aspirio Ltd. is responsible for ensuring that Aspirio Ltd.'s infrastructure/network is as safe and secure as possible and that policies and procedures approved within this policy are implemented. Aspirio Ltd. should ensure that all staff are regularly aware of policies and procedures and explain that everyone is responsible for online safety and data protection.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.



ASPIRIO

**Registered office : The Braes,
Granville Road, Bath. BA1 9BE**

Aspirio Ltd:

- ❖ Has a data protection policy
- ❖ Implements the data protection principles and can demonstrate that it does so
- ❖ Has appointed an appropriate Data Protection Officer (DPO) who has a practical understanding of data protection law and is free from any conflict of interest
- ❖ Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why, and which staff member is responsible for managing it.
- ❖ Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes for which it was collected.
- ❖ Data held is accurate and up to date and only for the purpose it was held for.
- ❖ Systems are in place to identify inaccuracies, such as asking parents/carers to check primary contact information at suitable intervals
- ❖ Provides mentors, mentees, and parents/carers with information about how Aspirio Ltd looks after their data and what their rights are in a clear Privacy Notice
- ❖ Has procedures in place to deal with the individual rights of the data subject
- ❖ Carries out Data Protection Impact Assessments where necessary
- ❖ Understands how to share data lawfully and safely with other relevant data controllers
- ❖ Has clear and understood policies and routines for the deletion and disposal of data
- ❖ Report any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- ❖ Has a Freedom of Information Policy which sets out how it will deal with FOI requests
- ❖ Provides data protection training for all staff at induction and appropriate refresher training thereafter.

When personal data is stored on any mobile device or removable media, the:

- ❖ Data will be password-protected and encrypted
- ❖ Device will be password protected
- ❖ Device will be protected by up-to-date anti-virus software
- ❖ Data will be securely deleted from the device, in line with Aspirio Ltd.'s policy, once it has been transferred or its use is complete

Mentors must ensure that they:

- ❖ At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- ❖ Can recognise a possible breach, understand the need for urgency and know who to report it to within Aspirio Ltd.
- ❖ Can help data subjects understand their rights, know how to handle a verbal or written request, and know who to pass it to in Aspirio Ltd.
- ❖ Transfer data using encryption, a secure email account, and secure password-protected devices



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

Aspirio Ltd should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that, in general terms, an illegal action, if committed offline, is also prohibited if committed online.

***ONLINE SAFETY ACT 2003: ***

This Act provides for a new regulatory framework with the general purpose of making Internet services safer for individuals. The purpose of this Act is to:

- ❖ Impose duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which mainly affect individuals with a particular characteristic) from illegal content and activity, and content and activity that is harmful to children
- ❖ Confer new functions and powers on the regulator, OFCOM
- ❖ Duties imposed on providers by this Act seek to secure (among other things) that services are safe by design and are designed and operated in such a way that a higher standard of protection is provided for children than for adults, users' rights to freedom of expression and privacy are protected, and transparency and accountability are provided about those services

Computer Misuse Act 1990

This Act makes it an offence to:

- ❖ Erase or amend data or programs without authority.
- ❖ Obtain unauthorised access to a computer.
- ❖ "Eavesdrop" on a computer.
- ❖ Make unauthorised use of computer time or facilities.
- ❖ Maliciously corrupt or erase data or programs.
- ❖ Deny access to authorised users.

The National Crime Agency website includes information about "Cybercrime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works to encourage young people to make positive use of their cyber skills. There is a helpful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of an individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- ❖ Fairly and lawfully processed.
- ❖ Processed for limited purposes.
- ❖ Adequate, relevant and not excessive.
- ❖ Accurate.



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

- ❖ Not kept longer than necessary.
- ❖ Processed by the data subject's rights.
- ❖ Secure.
- ❖ Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR)

And aims to:

- ❖ Facilitate the secure transfer of information within the European Union.
- ❖ Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives and business.
- ❖ Give the public confidence about how businesses can use their personal information.
- ❖ Provide data subjects with the legal right to check the information businesses hold about them. They can also request that the data controller destroy it.
- ❖ Give data subjects greater control over how data controllers handle their data.
- ❖ Place emphasis on accountability. This requires businesses to have processes demonstrating how they're securely handling data.
- ❖ Require firms to keep people's data safe and secure. Data controllers must ensure that it is not misused.
- ❖ Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- ❖ Receive clear information about what you will use their data for.
- ❖ Access their personal information.
- ❖ Request their data be revised if out of date or erased. These are known as the right to rectification and the right to erasure.
- ❖ Request information about the reasoning behind automated decisions, such as if computer software denies them access to a loan.
- ❖ Prevent or query about the automated processing of their data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow several set procedures.

Communications Act 2003

Sending using the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character or sending a false message using or persistently making use of the Internet to cause annoyance, inconvenience or needless anxiety is guilty of an offence liable, on



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

Conviction to imprisonment. This wording is important because an offence is complete, and as soon as the message has been sent, there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted to:

- ❖ Establish the facts.
- ❖ Ascertain compliance with regulatory or self-regulatory practices or procedures.
- ❖ Demonstrate standards which are or ought to be achieved by persons using the system.
- ❖ Investigate or detect unauthorised use of the communications system.
- ❖ Prevent or detect crime in the interests of national security.
- ❖ Ensure the effective operation of the system.
- ❖ Monitoring but not recording is also permissible to:
 - Ascertain whether the communication is business or personal.
 - Protect or support staff.
 - Aspirio reserves the right to monitor its systems and communications in line with its rights under this act.

Trademarks Act 1994

This protects Registered Trademarks, which can be any symbol (words, shapes or images) associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a confusing mark like an existing mark.

Copyright, Designs and Patents Act 1988

Copying all or a substantial part of a copyrighted work is an offence. There are, however, expressly limited user permissions, such as fair dealing, which means that under certain circumstances, permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, including words, images, sounds, moving images, TV broadcasts, and other media (e.g., YouTube).



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

Telecommunications Act 1984

It is an offence to send a message or other grossly offensive matter or of an indecent, obscene or menacing character. It is also an offence to send a message intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- ❖ Use threatening, abusive or insulting words or behaviour or disorderly behaviour OR
- ❖ Display any writing, sign or other visible representation that is threatening, abusive or insulting, thereby causing harassment, alarm or distress to that person or another person.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct that amounts to harassment of another and which they know or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions that violence will be used against them is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. A picture of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world to commit a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams for your gratification. It



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, and connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue or discrete subject area within the law. It is a type of "higher law" affecting all other laws. In the school context, human rights to be aware of include:

- ❖ The right to a fair trial
- ❖ The right to respect for private and family life, home and correspondence
- ❖ Freedom of thought, conscience and religion
- ❖ Freedom of expression
- ❖ Freedom of assembly
- ❖ Prohibition of discrimination
- ❖ The right to education

These rights are not absolute. The school must respect these rights and freedoms, balancing them against those rights, duties and obligations arising from other relevant legislation.

The Protection of Freedoms Act 2012

Requires permission from a parent/carers to use Biometric systems

Serious Crime Act 2015

Introduced a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)



ASPIRIO

Registered office : The Braes,
Granville Road, Bath. BA1 9BE

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent to cause them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

***CONTACT DETAILS: ***

Online safety co-ordinator and senior lead for safeguarding and child protection:

Name: Kylie Stewart

Phone/email: 07917755744 / kylie@aspirio.co.uk

NSPCC Helpline: 0808 800 5000

We are committed to reviewing our policy and good practice annually. This policy was last reviewed on 07.03.2025