



Online Safety and Mobile Phone Policy

Approved by:	Lauren Meston	Date: 01/09/2026
---------------------	---------------	-------------------------

Last reviewed on:	01/09/2026
--------------------------	------------

Next review due by:	31/08/2027
----------------------------	------------

Introduction:

Future Pathways is committed to providing a safe, respectful and purposeful learning environment in which technology is used to support education without exposing young people to avoidable online harm. Online safety is a safeguarding responsibility and is treated as part of our wider child protection, behaviour, anti-bullying, equality, data protection and curriculum arrangements.

Future Pathways is an alternative provision. Our approach reflects the individual needs and risk profiles of the young people we support, including those who may be vulnerable to exploitation, harmful online contact, cyberbullying, inappropriate content, coercion, fraud, radicalisation, image-based abuse or other technology-facilitated harm.

Young people at Future Pathways do not have access to mobile phones or other personal smart devices during the education day, including lessons, movement between activities, breaktimes and lunchtimes. Internet access for young people is provided only through Future Pathways-managed laptops. These devices are filtered and monitored and young people are supervised by staff at all times while using them.

Aims of this policy:

- protect young people from harmful, illegal and inappropriate online content, contact, conduct and commercial risks
- ensure technology is used safely, responsibly and only for legitimate educational purposes
- maintain a mobile-phone-free environment throughout the education day
- ensure all young-person internet access takes place through managed, filtered and monitored Future Pathways laptops
- ensure young people are actively supervised whenever they use internet-connected laptops
- make clear the responsibilities of staff, leaders, young people, parents/carers and partner organisations
- identify online safeguarding concerns quickly and ensure they are reported to the Designated Safeguarding Lead without delay
- maintain effective filtering and monitoring arrangements and review them at least annually
- support young people to build digital resilience, critical thinking and safe online behaviours
- respond consistently to misuse, while taking account of safeguarding, SEND, trauma and individual circumstances

Legal and guidance framework:

This policy has been developed with regard to current legislation and Department for Education guidance, including:

- Keeping Children Safe in Education 2026, in force from 1 September 2026
- Department for Education statutory guidance: Mobile phones in schools, statutory from 29 June 2026 and to be followed from 1 September 2026
- Department for Education: Meeting digital and technology standards in schools and colleges - Filtering and monitoring core standard, updated June 2026
- Working Together to Safeguard Children 2026

- Behaviour in Schools guidance, where applicable to the setting and commissioning arrangements
- Prevent duty guidance for England and Wales
- Education Act 2002 and relevant safeguarding duties, where applicable
- Children Act 1989 and Children Act 2004
- Equality Act 2010 and the requirement to make reasonable adjustments for disabled young people
- UK GDPR and Data Protection Act 2018
- Computer Misuse Act 1990, Communications Act 2003 and relevant criminal law relating to online conduct

Where a young person is placed by a commissioning school or local authority, Future Pathways will also follow relevant commissioning, safeguarding and information-sharing arrangements.

Online safety leadership and responsibilities:

Lauren Meston - Managing Director and Designated Safeguarding Lead (DSL)

Lauren Meston has overall organisational responsibility for safeguarding at Future Pathways. Any online incident that raises a child protection or safeguarding concern must be reported to the DSL promptly. The DSL is responsible for safeguarding decisions arising from online activity, including referrals to children's social care, police, Prevent or other agencies where required.

Pete Meston - Designated Online Safety Coordinator

Pete Meston is the designated Online Safety Coordinator and leads the day-to-day coordination of online safety arrangements. His responsibilities include:

- supporting implementation and annual review of this policy
- working with the DSL, senior leaders and IT support on filtering and monitoring
- coordinating regular checks that filtering and monitoring arrangements are operating as intended
- ensuring staff understand the procedures for reporting online concerns and technical failures
- supporting staff awareness and online safety training
- reviewing trends in online incidents and recommending improvements
- ensuring new devices and services are considered for safeguarding, filtering, monitoring and privacy risks before use
- maintaining oversight of acceptable-use expectations for young people and staff

The Online Safety Coordinator does not replace the DSL. Where an issue is or may be a safeguarding concern, the DSL must be informed and will determine the safeguarding response.

All staff

All staff are responsible for maintaining online safety in the activities they supervise. Staff must:

- maintain active supervision whenever young people use laptops or other authorised technology
- remain aware of what is visible on young people's screens and intervene where use is unsafe or inappropriate

- follow this policy, safeguarding procedures, staff code of conduct and acceptable-use requirements
- report online safeguarding concerns to the DSL without delay
- report filtering, monitoring or technical weaknesses to Pete Meston and/or the relevant IT support promptly
- never disable, bypass or encourage circumvention of filtering, monitoring or security controls
- use professional accounts, devices and communication methods for work-related contact with young people unless an authorised exception has been agreed
- model safe, respectful and lawful use of technology

The four areas of online risk:

Future Pathways recognises the four broad areas of online risk identified within safeguarding guidance: content, contact, conduct and commerce. These risks can overlap and may occur on social media, gaming services, messaging applications, websites, live-streaming platforms, AI tools or other digital services.

- Content - exposure to illegal, inappropriate or harmful material, including sexual content, violence, self-harm or suicide material, extremist content, misinformation, disinformation and harmful AI-generated content.
- Contact - harmful interaction with other users, including grooming, exploitation, coercion, harassment, sexual pressure, scams, radicalising contact or contact from unknown adults.
- Conduct - harmful online behaviour by a young person or towards a young person, including cyberbullying, abusive messages, sharing intimate images, discriminatory abuse, impersonation or encouraging harmful behaviour.
- Commerce - risks such as online gambling, financial scams, inappropriate advertising, phishing, fraudulent purchases or pressure to spend money.

Mobile phones and personal smart devices:

Future Pathways operates a clear mobile-phone-free policy for young people throughout the education day. This reflects Department for Education expectations that pupils should not have access to mobile phones during lessons, between lessons, breaktimes or lunchtime.

For the purpose of this policy, mobile phones also includes smartphones and other personal communication or smart technology capable of messaging, calling, internet access, photography, video, recording, social media or similar communication. This may include smart watches, internet-enabled wearable devices and personal tablets where applicable.

Future Pathways rules

- Young people must not have access to a smartphone or other prohibited personal smart device at any point during the education day, including breaktimes and lunchtimes.
- Where a young person brings a phone or prohibited smart device to Future Pathways, it must be handed to staff on arrival and stored securely in accordance with the setting's agreed arrangements until the young person leaves for the day.
- Young people must not retain a second phone, hidden device, smart watch or other communication device.
- Personal mobile data, personal hotspots, tethering, VPNs or proxy services must not be used to provide internet access on site.

- Young people must not use another person's phone or smart device while attending Future Pathways.
- Parents/carers who need to contact a young person during the education day should contact Future Pathways. Where a young person needs to contact home, staff will facilitate this through an authorised setting phone or other agreed arrangement.
- Phones are returned at the end of the young person's education day unless they are being retained temporarily in accordance with a lawful behaviour, safeguarding or evidence-preservation process.

Exceptions

Any exception must be individual, necessary, proportionate and formally authorised. An exception may be considered where a mobile or smart device is required because of a medical condition, disability, SEND need or another compelling safeguarding reason. Any agreed exception must be documented and risk assessed, with clear rules about when, where and how the device may be used. An exception will not provide unrestricted access to a personal smartphone.

Failure to follow the mobile phone rules

Where a young person refuses to hand in a device, accesses a prohibited device, or attempts to conceal or use one during the education day, staff will respond in line with the Behaviour Policy and individual risk assessment. Staff should avoid unnecessary confrontation and must consider whether the behaviour indicates a safeguarding issue, such as exploitation, coercion, harmful contact, threats, image-sharing or criminal activity.

Where an incident involves suspected criminal conduct, indecent or sexual images, threats, exploitation or other safeguarding concerns, the device must not be searched casually. Staff must preserve safety and evidence, inform the DSL and follow current safeguarding and searching/confiscation guidance.

Young people's access to the internet:

Young people are not permitted to access the internet through personal devices at Future Pathways. The only authorised internet access for young people is through Future Pathways-managed laptops provided for education.

The laptops are subject to filtering and monitoring controls. Young people are supervised by staff at all times while using them. Staff must remain actively aware of the activity taking place and must not rely solely on technical systems to keep young people safe.

Access is for educational purposes and must be appropriate to the activity being undertaken. Staff may restrict, pause or remove access where necessary to protect safety, maintain learning or investigate misuse.

Filtering and monitoring:

Future Pathways will maintain filtering and monitoring arrangements that are appropriate to the age, needs, SEND profile and safeguarding risk of the young people attending the provision. Filtering is used to prevent access to illegal, harmful or inappropriate content. Monitoring is used to identify concerning activity and support a timely response.

The Managing Director, DSL, Online Safety Coordinator and IT support will work together to ensure that responsibilities are clear and that filtering and monitoring systems are suitable for the setting.

Future Pathways will:

- filter all authorised young-person internet access on managed laptops
- block access, so far as reasonably practicable, to illegal child sexual abuse material, unlawful terrorist content, adult content and other content assessed as harmful or inappropriate
- take steps to block or restrict technologies intended to circumvent filtering, including VPNs, proxies and unauthorised personal hotspots
- maintain monitoring capable of identifying concerning activity and allowing incidents to be followed up promptly
- ensure users can be identified wherever reasonably practicable so concerns can be attributed and investigated
- carry out and record checks that filtering and monitoring systems remain active and effective
- review filtering and monitoring provision at least once every academic year, and sooner where technology, risk or incidents indicate a need
- consider the risks presented by generative AI, dynamic and personalised content, new platforms and new devices before they are introduced
- maintain a process for urgent escalation of high-risk monitoring alerts and safeguarding concerns
- ensure that technical monitoring complements, rather than replaces, active staff supervision

Any failure, suspected bypass or inappropriate gap in filtering or monitoring must be reported immediately to Pete Meston and the relevant IT support. Where the failure creates an immediate safeguarding risk, access to the affected device or service will be restricted until the risk is addressed.

Supervision of laptop use:

Young people must be supervised by a member of staff whenever using a Future Pathways laptop. Supervision should be active and proportionate to the activity and individual risk. Staff should position themselves so that screens can be viewed, maintain awareness of searches and websites being accessed, and intervene where behaviour or content gives cause for concern.

Where individual young people have heightened online risks, additional measures may include closer supervision, restricted websites or applications, individual user settings, shorter periods of access, direct staff support or a specific online-safety risk assessment.

Acceptable use by young people:

Young people using Future Pathways laptops are expected to:

- use devices only when authorised and for the activity directed by staff
- use their own assigned account where one is provided and keep login details private
- treat other people respectfully online and not engage in bullying, harassment, threats or discriminatory abuse
- not search for, create, download, upload, store or share illegal, sexual, violent, extremist or otherwise harmful content
- not attempt to bypass filtering, monitoring, account restrictions or network security
- not install software, browser extensions, games or applications without permission

- not use personal email, social media, messaging or gaming services unless specifically authorised for a legitimate educational purpose
- not photograph, film or record another person without permission and a legitimate educational reason
- not access or interfere with another user's files, accounts or communications
- tell a member of staff immediately if they see something online that worries, frightens or upsets them or if someone contacts them inappropriately

Social media, messaging and online communication:

Young people do not have access to personal smartphones during the Future Pathways day and should not use Future Pathways laptops to access personal social media, messaging or private communication services unless a specific educational activity has been authorised and risk assessed.

Staff must maintain professional boundaries online. Staff must not use personal social media accounts or personal messaging accounts to communicate privately with young people. Any authorised electronic communication with young people must use approved systems and comply with the Staff Code of Conduct and safeguarding procedures.

Online behaviour occurring outside Future Pathways may still require action where it affects the safety, wellbeing or education of a young person, creates a risk within the provision, involves members of the Future Pathways community, or constitutes a safeguarding concern.

Cyberbullying, discrimination and harmful peer behaviour:

Cyberbullying, online harassment, discriminatory abuse, sexual harassment, threats, coercion, image-based abuse and other harmful online behaviour will be taken seriously. Staff must not dismiss harmful online behaviour as banter, drama or something that happened outside the provision.

Incidents will be considered under the Anti-Bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy as appropriate. Where online behaviour may constitute child-on-child abuse, sexual violence or harassment, exploitation, hate crime or another safeguarding risk, the DSL will lead or oversee the response.

Sharing of sexual or indecent images:

Any concern involving the creation, request, possession or sharing of nude or semi-nude images or videos involving a child must be treated as a safeguarding matter. Staff must not ask a young person to forward an image, must not copy or print it and should not intentionally view the image unless this is unavoidable in the course of receiving the report.

The device should be secured where necessary, the DSL informed immediately, and the incident managed in line with current safeguarding guidance on sharing nudes and semi-nudes. Police or children's social care involvement will be considered according to the nature and level of risk.

Online exploitation, radicalisation and criminal risk:

Staff should be alert to technology being used to facilitate criminal or sexual exploitation, county lines activity, blackmail, coercive control, fraud, radicalisation, extremist influence or contact with unsafe adults. Changes in device secrecy, unexplained money, threats,

pressure to communicate, persistent unknown contacts or attempts to regain phone access may be relevant indicators and should be considered with professional curiosity.

Concerns must be reported to the DSL without delay. Where there is an immediate risk of serious harm or a crime in progress, staff should contact emergency services in accordance with safeguarding procedures.

Generative artificial intelligence (AI):

Future Pathways recognises that generative AI tools can create educational opportunities but may also generate inaccurate, harmful, biased, sexual, extremist, manipulated or otherwise inappropriate content. They may also create privacy, intellectual-property and safeguarding risks.

Young people may only use generative AI tools where specifically authorised and supervised by staff using approved devices and services. Staff must consider whether the service is suitable, whether personal data may be entered, whether content is appropriately filtered and monitored, and whether outputs require verification. Young people must not use AI to create harmful, abusive, sexualised, deceptive or impersonating content.

Data protection, privacy and monitoring transparency:

Future Pathways will process monitoring and safeguarding information in accordance with data-protection law. Monitoring will be proportionate to safeguarding and operational needs. Relevant privacy information will explain that activity on Future Pathways systems and devices may be filtered, logged and monitored.

Where a technical monitoring service is used, Future Pathways will consider data-protection requirements, including the need for appropriate privacy information and a Data Protection Impact Assessment where required. Monitoring information will be accessible only to authorised staff and will be retained and shared in accordance with safeguarding, data protection and records-management requirements.

Staff use of devices and technology:

Staff use of phones, cameras, laptops and communication systems must comply with the Staff Code of Conduct and safeguarding expectations. Personal devices must not be used in a way that undermines the mobile-phone-free environment, distracts from supervision or creates inappropriate contact with young people.

Staff must not take photographs or recordings of young people on personal devices unless an exceptional authorised arrangement is in place and all safeguarding and data-protection requirements have been addressed. Work-related photographs and recordings must use approved devices and systems.

Responding to an online safety incident:

1. Make the situation safe. Stop or restrict the activity where necessary without destroying potential evidence.
2. Listen to the young person and take the concern seriously. Do not promise confidentiality.
3. If there is an immediate risk of serious harm, contact emergency services as appropriate and inform the DSL.

4. Report any safeguarding element to Lauren Meston, DSL, without delay. Inform Pete Meston, Online Safety Coordinator, where appropriate for technical or online-safety follow-up.
5. Record what was reported or observed factually, including the device, website, account, time and any action already taken.
6. Do not investigate beyond your role. Do not deliberately search for illegal material or ask a young person to reproduce or forward harmful content.
7. Preserve relevant evidence in a safe and lawful way where this can be done without further viewing, copying or sharing harmful material.
8. Follow safeguarding, behaviour, anti-bullying, police or external referral procedures as directed by the DSL.
9. Review whether filtering, monitoring, supervision, risk assessment or individual support needs to change following the incident.

Search, confiscation and preservation of devices:

Any search, confiscation or examination of a device must be lawful, necessary and proportionate and must follow current Department for Education guidance and Future Pathways procedures. Staff should be particularly cautious where a device may contain sexual images, evidence of exploitation, threats, illegal content or other material that could be compromised by unnecessary access.

Where there is doubt, staff should secure the situation and seek advice from the DSL rather than searching content themselves. Devices may need to be preserved for police or safeguarding purposes.

Parents, carers and commissioning schools:

Future Pathways will communicate the mobile-phone-free rule and key online-safety expectations to parents/carers and commissioning schools. Parents/carers are asked not to contact young people directly on a mobile phone during the education day and should use Future Pathways as the point of contact where an urgent message is required.

Where online incidents affect safeguarding, attendance, behaviour or placement stability, relevant information will be shared with parents/carers, commissioning schools, local authorities or other agencies on a proportionate need-to-know basis, subject to safeguarding and data-protection considerations.

Education and digital resilience:

Restricting access to personal smartphones does not remove the need to teach young people how to navigate online risks. Future Pathways will provide age-appropriate and needs-led online-safety education through curriculum, safeguarding work, pastoral support and individual intervention where appropriate.

Education may include online relationships, consent, privacy, scams, misinformation, digital footprints, cyberbullying, sexual image-sharing, exploitation, radicalisation, AI-generated content, respectful communication and how to seek help.

Training and staff awareness:

Staff will receive appropriate online-safety information and training as part of safeguarding induction and ongoing updates. Training will include the mobile-phone policy, active

supervision, filtering and monitoring responsibilities, reporting routes, online child protection risks and how to respond to harmful content or disclosures.

Pete Meston will support online-safety awareness, while safeguarding decisions and child protection training remain under the oversight of the DSL.

Monitoring, audit and review:

Future Pathways will review its filtering and monitoring provision at least once every academic year and will record the outcome. The review will involve senior leadership, the DSL, Pete Meston as Online Safety Coordinator and relevant IT support. It will consider the young people's risk profile, current technology, incident patterns, emerging risks, staff practice, new devices/services and any weaknesses identified through checks or alerts.

Filtering and monitoring checks will be recorded. The frequency of checks will be based on risk, but they must be sufficient to confirm that systems have not been disabled or misconfigured and that the correct controls apply to young-person devices and accounts.

This policy will be reviewed at least annually and sooner where there is a serious online-safety incident, significant change in technology, change in statutory guidance, failure of filtering or monitoring, or evidence that existing arrangements are not effective.

Related Future Pathways policies and documents:

- Safeguarding and Child Protection Policy
- Low-Level Concerns Policy
- Anti-Bullying Policy
- Behaviour Policy
- Attendance Policy
- Absconding / Leaving Without Permission Policy
- SEND Policy
- Equality and Diversity Policy
- Staff Code of Conduct
- Data Protection and Privacy Policies
- Acceptable Use Agreement
- Educational Visits Policy
- Risk Assessment procedures
- Whistleblowing Policy

Appendix 1 - Staff quick guide:

Young people at Future Pathways:

- must not have access to a smartphone or prohibited smart device at any time during the education day, including breaks and lunch
- must hand in any phone or prohibited smart device on arrival for secure storage
- may access the internet only through Future Pathways-managed laptops
- must be supervised by staff at all times when using laptops
- must not use hotspots, mobile data, VPNs, proxies or other methods to bypass the Future Pathways network or filters

If you see or receive an online-safety concern:

- make the situation safe and do not destroy evidence
- do not ask a young person to forward or reproduce harmful or sexual content

- report safeguarding concerns to Lauren Meston, DSL, immediately
- inform Pete Meston, Online Safety Coordinator, about relevant technical or online-safety issues
- record the facts promptly
- if there is immediate danger, call 999 and inform the DSL

Appendix 2 - Online safety incident record:

Young person(s):

Date and time:

Location / activity:

Device used:

Website / service / platform:

What was observed or reported:

Immediate safety action taken:

Safeguarding concern identified:

DSL informed - date/time:

Online Safety Coordinator informed - date/time:

Parent/carer informed:

Commissioning school informed:

External agencies / police involved:

Evidence preserved and how:

Filtering / monitoring issue identified:

Action required:

Outcome / follow-up:

Recorded by and date:

Appendix 3 - Filtering and monitoring review checklist:

- Roles and responsibilities for filtering and monitoring are documented and understood.
- All Future Pathways-managed laptops used by young people are covered by filtering and monitoring.
- User groups and accounts apply the correct level of filtering.
- Illegal child sexual abuse material, unlawful terrorist content and adult content are blocked as a minimum.
- VPNs, proxies, unauthorised hotspots and other circumvention techniques are restricted so far as reasonably practicable.
- Monitoring can identify concerning activity and supports prompt escalation of high-risk incidents.
- Staff know how to report filtering failures, monitoring alerts and online safeguarding concerns.
- Checks are recorded with date, person completing the check, what was tested and any resulting action.
- New devices, applications, AI tools and services are assessed before young-person use.
- Monitoring and filtering arrangements reflect the current cohort, SEND needs and known safeguarding risks.
- Privacy information and data-protection requirements for monitoring systems have been considered.
- The annual filtering and monitoring review has been completed and actions have been recorded.

Approval:

Signed: *L. Meston*

Lauren Meston - Managing Director and Designated Safeguarding Lead, Future Pathways

Pete Meston - Designated Online Safety Coordinator, Future Pathways

Date: 16/08/2026

Next review due: 31/08/2027