Online Safety Policy

Document Control:

Policy Owner	Designated Safeguarding Lead (DSL), Julia Bindley
Policy Author(s)	Safeguarding Lead (DDSL), Sean Thomson
Effective Date	15 October 2026
Version Number	[V2]
Date of Next Review	1st October 2027

Amendment History:

Version Number	Effective Date	Summary of Amendments	Author
[V1.0]	01.10.25	First version	Safeguarding Implementation Lead, Jemma Ansell
[V1.1]	23.03.26	Online Safety Incident Flowchart Update	Safeguarding Lead (DDSL), Sean Thomson
[V2]	15.10.26	Annual review. Aligned to updated Safeguarding Policy V7.0 and KCSIE 2026. Added statutory framework list. Updated AI governance and incident routing (including new Crime and Policing Act 2026 offences). Documentation of expansion of Online Safety Group membership. Strengthened acceptable use provisions for AI-generated imagery. Updated legislative references throughout. Online Safety Incident Flowchart Update.	Safeguarding Lead (DDSL), Sean Thomson

© Multiverse 2026

1. Policy Introduction & Statement

1.1 This Online Safety Policy outlines the commitment of Multiverse to safeguard members of its community online in accordance with statutory guidance and best practice. Multiverse will deal with such incidents within this policy and associated conduct and disciplinary policies, and will, where applicable, inform parents/carers of incidents of inappropriate online safety behaviour if an individual engaged in that behaviour is a child (under 18).

1.2 This policy is informed by, and should be read alongside, the following legislation and guidance:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Online Safety Act 2023
- Crime and Policing Act 2026 (including the section 46A offence relating to CSA image generators)
- Data Protection Act 2018 / UK GDPR / Data (Use and Access) Act 2025
- Information Sharing Duty 2026
- Prevent Duty Guidance (Home Office, 2023)
- The Prevent Duty: Practical Guidance For Designated Safeguarding Leads (DfE, September 2026)
- DfE Filtering and Monitoring Standards (updated June 2026)
- DfE Generative AI Product Safety Standards (January 2026)
- Multiverse Safeguarding Policy (V7.0, October 2026)

This policy should be read in conjunction with the Multiverse Safeguarding Policy, the Devices and Acceptable Use Policy (internal only), the Data Security Policy (internal only), and the Staff Disciplinary Policy (internal only).

2. Policy Scope

This policy applies to all members of the Multiverse community (including staff, learners, parents/carers of under 18s, visitors) who have access to and are users of Multiverse digital systems, both in and out of the office.

© Multiverse 2026

3. Policy Development, Monitoring and Review

3.1. The original version of this Online Safety Policy was developed by Multiverse's Online Safety Group made up of:

- The Designated Safeguarding Lead (DSL)
- The Deputy Designated Safeguarding Lead (DDSL)
- Head of Enterprise Technology

3.2. The schedule for the policy's development, monitoring and review is detailed in the table below:

This Online Safety Policy was approved by Multiverse's Online Safety Group on:	10/10/2025
The implementation of this Online Safety Policy will be monitored by:	The Online Safety Group
Monitoring will take place at regular intervals:	Quarterly
The Quality Sub-Committee will receive an update on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Quarterly
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments , new threats to online safety,relevant legislative or regulatory changes, or incidents that have taken place. In line with the DfE Filtering and Monitoring Standards (updated June 2026), the introduction of any new AI tool will trigger an immediate out-of-cycle review of the filtering and monitoring provision. The next anticipated review date will be:	September 2026

4. Process for Monitoring the Impact of the Online Safety Policy

4.1. Multiverse will monitor the impact of the policy using:

- Logs of reported incidents.
- Relevant filtering and monitoring logs.
- Staff training reviews, and knowledge gap analysis.
- Relevant external guidance and law updates.

© Multiverse 2026

5. Roles and Responsibilities

5.1. CEO and Exec team members

- The CEO has a duty of care for ensuring the safety (including online safety) of members of the Multiverse Community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the DSL, as defined in Keeping Children Safe in Education (KCSIE) 2026.
- The CEO and the Exec team members should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The CEO and the Exec team members are responsible for ensuring that the DSL, Head of Enterprise Technology and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The CEO and the Exec team members will ensure that there is a system in place to allow for monitoring and support of those in Multiverse who carry out the internal online safety monitoring role.
- The CEO and the Exec team members will receive an annual report from the Online Safety Group.
- The CEO and the Exec team members will ensure the responsible Governor, the Designated Safeguarding Lead (DSL) and the Head of Enterprise Technology have what they require for all aspects of filtering and monitoring.

5.2. Lead Governor for Safeguarding

- Governor is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- This review will be carried out by the Quality Sub-Committee whose members will receive information quarterly about online safety incidents and monitoring reports. The Lead Governor for Safeguarding will take on the role of Online Safety Governor to include:
- regular meetings with the DSL,
- regularly receiving (collated and anonymised) reports of online safety incidents,
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended),
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually,
- receiving sufficient training to enable the Governor to check that Multiverse meets the DfE Standards.

5.3. Designated Safeguarding Lead (DSL)

- The DSL holds the lead responsibility for online safety, within their safeguarding role.
- The DSL should receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online

© Multiverse 2026

- The DSL should meet regularly with the Lead Governor for Safeguarding to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that quarterly filtering and monitoring checks are carried out.
- The DSL should attend the Quality Sub-Committee on a quarterly basis.
- The DSL should report regularly to the CEO and Exec team members.
- The DSL is ultimately responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- In the absence of the DSL, the DDSL will act as the lead for online safety matters, including incident decision-making, in accordance with the DSL Cover and Absence SOP set out in the Safeguarding Policy.

5.4. The Deputy Designated Safeguarding Lead (DDSL)

- The DDSL leads the coordination of the Online Safety Group.
- The DDSL works closely on a day-to-day basis with the DSL.
- The DDSL receives reports of online safety issues, being aware of the potential for serious child protection concerns and ensures that these are logged to inform future online safety developments.
- The DDSL has a leading role in establishing and reviewing the online safety policies/documents
- The DDSL promotes an awareness of and commitment to online safety education / awareness raising across Multiverse.
- The DDSL ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- The DDSL provides (or identifies sources of) training and advice for staff/governors/parents/carers/learners
- The DDSL receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined in KCSIE 2026: content, contact, conduct and commerce.

5.5. All Staff

- All staff have an awareness of current online safety matters/trends and of the current Online Safety Policy and practices.
- All staff understand that online safety is a core part of safeguarding.
- All staff have read, understood, and signed the Devices and Acceptable Use Policy as part of their employment contracts.
- All staff follow all relevant guidance and legislation including, for example, n KCSIE 2026 (for staff carrying out Regulated Activity) and UK GDPR regulations (for all staff).
- All digital communications with learners should be on a professional level and only carried out using official Multiverse systems and devices (where staff use AI, they must only use tools within Multiverse's Authorised Tech Stack, which have been evaluated against DfE Generative AI Product Safety Standards (January 2026) and Multiverse's organisational security and oversight requirements). Staff must not use any AI tool - whether Multiverse-approved

© Multiverse 2026

or personal - to create, alter or manipulate sexual, nude or semi-nude imagery of any person. This is a criminal offence under the Crime and Policing Act 2026 (section 46A) in addition to being gross misconduct.
- All staff immediately report any suspected misuse or problem to the Safeguarding Team (safeguarding@multiverse.io) for investigation/action, in line with safeguarding procedures.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- All staff model safe, responsible, and professional online behaviours in their own use of technology, including out of work and in their use of social media.
- All staff adhere to Multiverse's cyber security and data protection policies, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity.
- All staff are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in education, being transparent in how they use these services, and prioritising human oversight. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked,critically evaluated and in line with our AI principles.

6. Online Safety Group

The Online Safety Group has the responsibility of overseeing issues regarding online safety and monitoring the Online Safety Policy, including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and governors.

6.1. The Online Safety Group has the following members:

- The Designated Safeguarding Lead (DSL) Chair
- The Deputy Designated Safeguarding Lead (DDSL)
- Head of Enterprise Technology
- Senior Legal Director
- Data Protection Officer
- Information Security Manager

The expanded membership reflects the increasing intersection of online safety with legal, compliance, data protection, and information security - particularly in relation to AI governance, the Crime and Policing Act 2026, and the DfE Generative AI Product Safety Standards.

6.2. Members of the Online Safety Group will assist the DSL and Deputy DSL with:

- The production/ review/ monitoring of the Online Safety Policy.
- The production/review/monitoring of the filtering procedures and requests for filtering changes.
- The mapping and reviewing the online safety education provision, ensuring relevance, breadth and progression and coverage.
- Reviewing filtering/monitoring/incident logs.

© Multiverse 2026

- Reviewing Community Hub moderation incident logs.
- Conducting an annual organisational Online Safety Risk Assessment
- Monitoring improvement actions identified through use of the risk assessment.
- Reviewing and approving any new AI tool before it is added to the Authorised Tech Stack, ensuring it meets the DfE Generative AI Product Safety Standards (January 2026) and Multiverse's data protection and security requirements.
- Conducting an immediate out-of-cycle review of the filtering and monitoring provision, in accordance with the DfE Filtering and Monitoring Standards (updated June 2026).
- Ensuring the Online Safety Group's remit encompasses the four categories of online risk set out in KCSIE 2026: content, contact, conduct and commerce.

6.3. The Online Safety Group meets quarterly, reporting their findings and subsequent actions to the Quality Sub-Committee.

7. Acceptable Use

Multiverse has defined what it regards as acceptable/ unacceptable use and this is shown in both the table below and the overarching Devices and Acceptable Use Policy (internal link only)

7.1. The Online Safety Policy will be reinforced through:

- Flying Start Meetings (for learners).
- New employee contracts.
- Multiverse Internal Knowledge Hub .
- Online Safety Training.
- Internal communications.
- Multiverse website.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & Illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	Any illegal activity for example: • Child sexual abuse imagery (CSAM) • 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					X

© Multiverse 2026

comments that contain or relate to:	of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering • Technical information, encryption software or technology, in violation of international or regional export control laws • Making, adapting, possessing, supplying or offering to supply a CSA image generator - any AI model, software or tool capable of generating CSAM, whether or not it depicts a real child (Crime and Policing Act 2026, section 46A) • Creating, sharing or possessing AI-generated, deepfake or digitally altered sexual, nude or semi-nude imagery of any person without their consent • Using any tool (including personal or non-Multiverse-approved tools) to create sexual, nude or semi-nude imagery of a learner - real, AI-generated, or digitally altered					
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					X

© Multiverse 2026

	access to Multiverse networks, data and files, through the use of 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 through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in Multiverse policies:	Accessing inappropriate material/activities online on a Multiverse device or in a Multiverse setting including pornography, gambling, drugs. (Informed by Multiverse's filtering practices)				X	
	Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy.)				X	
	Offensive or obscene material which is likely to cause embarrassment to us or to our clients				X	
	A false and defamatory statement about any person or organisation				X	

© Multiverse 2026

	Access or share confidential information about Multiverse or any Multiverse Personnel or clients (except as authorised in the proper performance of duties)				X	
	Creating, sharing, or amplifying misinformation, disinformation, or conspiracy content through Multiverse systems or in Multiverse settings, where this could cause harm to learners, staff or the wider community - including content generated or amplified by AI tools				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by Multiverse				X	

8. Reporting and Responding

Multiverse will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of Multiverse settings, which may require intervention.

8.1. Multiverse will ensure:

- There are clear reporting routes which are understood and followed by all members of the Multiverse community which are consistent with the safeguarding procedures.
- All members of the Multiverse community will be made aware of the need to report online safety incidents. Learners will be informed during their Flying Start, whilst staff will be informed via their contracts, the Multiverse Internal Knowledge Hub and for those engaging in Regulated Activity, through mandatory Online Safety Training.
- Reports will be dealt with as soon as is practically possible once they are

© Multiverse 2026

received.

- The DSL, DDSL and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed safeguarding procedures.
- Any concern about staff misuse will be reported to the People Team, unless the concern involves members of the People Team or CEO, in which case the complaint is referred to the Governors.
- Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.
- All information-sharing decisions arising from online safety incidents - including decisions about whether to inform parents of under 18s, carers, employers or other third parties - are governed by the confidentiality and information-sharing framework set out in the Safeguarding Policy. For adult learners, this distinguishes between adults at risk and adults not at risk with capacity; the rules on sharing information without consent differ materially between the two categories, and staff must apply the Safeguarding Policy's framework rather than making an independent judgement under this policy alone.
- In accordance with the Information Sharing Duty 2026, Multiverse will share information about learners under 18 with relevant safeguarding partners wherever this is relevant to safeguarding or promoting their welfare, as set out in the Safeguarding Policy.
- Where an online safety concern meets the threshold for 'Harm' as defined in the Safeguarding Policy and involves a member of staff, the referral duties set out in the Safeguarding Policy apply - including referral to the Disclosure and Barring Service (DBS) and/or the Teaching Regulation Agency (TRA) where the criteria are met. This applies regardless of whether the incident originated as an 'online safety' or a 'safeguarding' report.

8.2. AI-Generated, Deepfake or Digitally Altered Imagery:

Where an online safety incident involves AI-generated, Deepfake or digitally altered sexual, nude or semi-nude imagery, staff must follow the escalation protocol set out in the Safeguarding Policy in full. This includes the requirements to stop and report immediately, preserve evidence, obtain DSL authorisation before any third-party notification, and not conduct any parallel internal investigation where a statutory agency is involved.

Where AI-generated child sexual abuse material (CSAM) is identified, external reporting routes include the Internet Watch Foundation (IWF) and NCA-CEOP, in addition to the police referral set out in the Safeguarding Policy.

The creation of AI-generated CSAM is a criminal offence under the Crime and

© Multiverse 2026

Policing Act 2026 (section 46A).

8.3. Where there is no suspected illegal activity, devices may be checked using the following procedure:

- The Online Safety Group will conduct this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected).
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following: internal response or discipline procedures, involvement by local authority, police involvement and/or action.
- Incidents and all actions taken will be logged in the Safeguarding Case Management System.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

The flowchart in Appendix One is available to staff to support the decision-making process for dealing with online safety incidents.

The information required for an Incident Report Log is stipulated in Appendix Two and should be recorded on the Safeguarding Case Management System when the process detailed in Section 8.3 is followed.

8.4. Learning from the incident, or pattern of incidents will be provided (as relevant and anonymously) to:

- The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
- Governors and Senior Leaders via the quarterly Quality Sub-Committee.
- Relevant staff through internal communications.
- Local authorities/ external agencies where relevant.
- Learners through internal communications, awareness raising or message reinforcements.

© Multiverse 2026

9. The Use of Artificial Intelligence (AI) at Multiverse

As generative Artificial Intelligence (GenAI) tools continue to advance and influence the world we live in, its role in education is evolving. Multiverse acknowledges the inherent risks associated with GenAI tools and services. However, these risks can be minimised by adapting our existing policies and procedures. The safeguarding of staff and learners will remain central to our policy and practice.

9.1. Multiverse acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing our team and our learners for a future in which AI technology will be an integral part.

Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

9.2. Multiverse will comply with all relevant legislation and guidance, with reference to KCSIE 2026, UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, and the Crime and Policing Act 2026. Multiverse's evaluation and approval of AI tools is informed by the DfE Generative AI Product Safety Standards (January 2026), which set out 13 minimum requirements an AI product must meet to be considered safe for use in an educational setting.

9.3. Multiverse will provide relevant training for staff in the advantages, use of and potential risks of AI. Multiverse will support staff in identifying training and development needs to enable relevant opportunities.

9.4. Multiverse will seek to embed learning about AI as appropriate in our programme content, including supporting learners to understand how GenAI works, alongside potential benefits, risks, and ethical / social concerns.

Multiverse recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

9.5. As set out in the Devices and Acceptable Use Policy, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data.

9.6. Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. Multiverse maintains an ‘Authorised Tech Stack’ within which we have an ‘AI walled garden’ containing tools that adhere to our IT standards. Staff are instructed to use only Multiverse-provided AI tools for work purposes. These tools have been approved for compliance with organisational security and oversight requirements, reducing the risk of data breaches.

9.7 Before any AI tool is added to the ‘Authorised Tech Stack’, it must be reviewed by the Privacy Team against the DfE Generative AI Product Safety Standards (January 2026). The introduction of a new AI tool will also trigger an immediate

© Multiverse 2026

out-of-cycle review of the filtering and monitoring provision, in accordance with the DfE Filtering and Monitoring Standards (updated June 2026). Records of AI tool evaluations and approval decisions will be collated for reporting purposes by the Safeguarding Team.

9.8. Multiverse will protect learner and customer data as required by law and our contractual obligations.

9.9. All AI-related incidents must be reported promptly. Quick reporting helps mitigate risks and facilitates a prompt response. Staff should not attempt to investigate AI incidents themselves before reporting. The reporting route depends on the nature of the incident:

- **Safeguarding concerns** - any incident involving AI-generated, deep fake or digitally altered imagery of a person; any AI output that raises a safeguarding concern about a learner or staff member; any use of AI tools to groom, harass, bully or exploit - must be reported immediately to the Safeguarding Team at safeguarding@multiverse.io. The Safeguarding Team will triage the incident and, where appropriate, refer to the Data Protection Team, Information Security, or other internal teams.
- **Data protection and security incidents** - data breaches involving AI tools, unauthorised processing of personal data by AI, or security vulnerabilities in AI systems - should be reported to the Data Protection Team at privacy@multiverse.io in accordance with the Incident Management Policy.
- **Other AI misuse** - use of non-approved AI tools, failure to disclose AI use where required, or generation of inappropriate (but non-safeguarding) outputs - should be reported to the line manager and, where the misuse involves a learner, to the Safeguarding Team.

9.10. AI tools may be used to assist staff in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Staff may also support learners to gain feedback on their own work using AI.

9.11. Multiverse will ensure human oversight when appropriate. Staff must ensure that AI-generated outputs are critically evaluated when concerns are raised.

9.12. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

9.13. The Crime and Policing Act 2026 (section 46A) makes it a criminal offence to make, adapt, possess, supply or offer to supply a 'CSA image generator - any AI model or tool (including CGI software) optimised or capable of generating CSAM, whether or not it depicts a real child. The prohibition on using any tool to create sexual, nude or semi-nude imagery of a learner applies regardless of which tool is used - including personal devices and non-Multiverse-approved tools - and regardless of whether the imagery is intended to be shared. This is a criminal offence, not solely a policy breach, and will be treated accordingly.

© Multiverse 2026

10. Online Safety Education Programme

10.1. Staff

All staff engaging or potentially engaging in Regulated Activity, as defined in Multiverse's Safer Recruitment Policy, will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A bespoke online safety e-learning module will be mandatory for stipulated staff to complete every 2 years. This e-learning module will be reviewed and accordingly updated annually by the Online Safety Group. The module will include, as a minimum: the recognition and reporting of AI-generated, deepfake and digitally altered imagery; online misogyny; the four categories of online risk (content, contact, conduct and commerce) as defined in KCSIE 2026; and the reporting routes set out in this policy.
- All Multiverse staff are mandated to complete GDPR UK Essentials Training and Cyber Security Awareness Training as part of their induction, and on an annual basis.
- Updates on online safety will be communicated internally to relevant staff through appropriate communication channels.
- The DSL and DDSL will receive regular updates on online safety at external training events and by reviewing updated guidance documents released by relevant organisations.
- The Safeguarding Team will provide advice and guidance to individuals as required.

Online safety education and awareness raising will take account of the needs of learners at potential greater risk of (online-based) harm, abuse, exploitation or scams, as identified in the Safeguarding Policy - including, but not limited to, LGBTQIA+ and Gender-questioning learners, care-leavers, and asylum seekers and refugees. Messaging will be tailored where appropriate to address the specific online risks these cohorts may face.

10.2. Governors

All governors will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A bespoke online safety e-learning module will be mandatory for governors to complete every 2 years. This e-learning module will be reviewed, and accordingly updated annually by the Online Safety Group.
- Governors are mandated to complete GDPR UK Essentials Training and Cyber Security Awareness Training as part of their induction and refreshed on an annual basis.

10.3. Mobile Phone Use

KCSIE 2026 introduces an expectation that schools/education providers operate a phone-free-by-default policy from 1 September 2026. This expectation is written for children in a school and classroom context. Multiverse's delivery model is

© Multiverse 2026

(predominantly) adult, workplace-based apprenticeships; learners use their own and employer-provided devices as part of their work and learning. Multiverse has considered this guidance and concluded that a blanket phone-free policy is not applicable to its delivery model. Multiverse's approach to mobile device use for staff is set out in the Devices and Acceptable Use Policy and section 13 of this policy.

11. Filtering and Monitoring

Multiverse has a statutory responsibility to ensure that appropriate filtering and monitoring systems are in place, as detailed in the KCSIE 2026 guidance.

Multiverse's filtering and monitoring provision is agreed by senior leaders, governors and the Head of Enterprise Technology and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents.

Checks on the filtering and monitoring system are carried out by the Head of Enterprise Technology. Individual concerns or incidents should be escalated by the Head of Enterprise Technology to the Safeguarding Team without delay. Overarching concerns with the suitability of the system should be raised by the Head of Enterprise Technology to the Online Safety Group and senior leaders to be addressed.

In accordance with the DfE Filtering and Monitoring Standards (updated June 2026), the introduction of any new AI tool into Multiverse's 'Authorised Tech Stack' will trigger an immediate out-of-cycle review of the filtering and monitoring provision, in addition to the annual review cycle.

11.1. Filtering

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

11.1.1. The Head of Enterprise Technology and the DSL, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties.

Role	**Responsibility**
Enterprise Technology	Ownership of all MV issued devices and authorised systems
WeWork	Network management for in office connections
Webroot	Web filtering and anti virus system

© Multiverse 2026

11.1.2. Multiverse manages access to content across its systems and devices for all users, and on all devices using the Multiverse internet provision in the office. The filtering provided meets the standards defined in the DfE Filtering Standards and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

11.1.3. Illegal content (e.g. CSAM) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

11.1.4 Where AI-generated CSAM is identified through filtering or monitoring, this must be reported immediately to the Safeguarding Team. External reporting routes include the Internet Watch Foundation (IWF), NCA-CEOP, and the police, in addition to the referral pathways set out in the Safeguarding Policy. Staff must not attempt to view, copy or retain the material.

11.1.5. There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures

11.1.6. There is a clear process in place to deal with, and log, requests/approvals for filtering changes.

11.1.7. Filtering logs are regularly reviewed by the Head of Enterprise Technology, and results are brought to Online Safety Group on a quarterly basis, where the DSL is informed of flagged incidents, and potential breaches to the Online Safety policy.

11.1.8. There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least quarterly and the results recorded and analysed to inform and improve provision. The findings are reported to the Online Safety Group.

11.1.9. Devices that are provided by Multiverse have Multiverse-based filtering applied irrespective of their location.

11.1.10. Multiverse details its approach to personal mobile devices being used in the Devices and Acceptable Use Policy, and where personal mobile devices have internet access through theWeWork Network, content is managed in ways that are consistent with Multiverse policy and practice.

11.1.11. Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with Multiverse policy and practice.

11.2. Monitoring

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

© Multiverse 2026

11.2.1. Multiverse has monitoring systems in place, agreed by senior leaders and technical staff, to protect Multiverse, systems and users. These systems follow the UK Safer Internet Appropriate Monitoring guidance.

11.2.2. Monitoring Safeguarding concerns are responded to with the necessary urgency, acted on, and outcomes are recorded by the DSL, all users are aware that monitoring is in place.

11.2.3. The monitoring provision is reviewed at least once every year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by a member of the Online Safety Group. The results of the review will be recorded and reported as relevant to the Quality Sub-Committee.

11.2.4. The monitoring provision will have particular regard to online radicalisation. The Home Office notes that most terrorism offences committed by young people now relate to online activity, such as possessing or sharing terrorist material. Monitoring should be alert to indicators of radicalisation and extremist content, in line with the Prevent Duty Guidance (2023) and its theme of reducing permissive environments. Any concerns should be escalated to the Safeguarding Team in line with the Safeguarding and Prevent Policies.

11.2.5. Devices that are provided by Multiverse have Multiverse-based monitoring applied irrespective of their location.

11.2.6. Where AI - supported monitoring is used, the purpose and scope of this is clearly communicated.

12. Information and Technical Security

Detailed Information and Technical Security Policies are outlined below:

12.1. Information Security Policy

12.2. Devices and Acceptable Use Policy

13. Mobile Technologies

The Devices and Acceptable Use Policy, alongside this Online Safety Policy details the expectations set by Multiverse around the use by staff of mobile technologies. This covers both personal devices used on Multiverse networks and Multiverse-provided devices. For Multiverse's position on the KCSIE 2026 phone-free-by-default expectation, see section 10.3.

14. Social Media

A clear Social Media Policy is in place that stipulates how staff should and should

© Multiverse 2026

not use social media, to ensure the safety of Multiverse learners and staff, alongside maintaining the integrity of Multiverse.

15. Digital and Video Images

15.1. Multiverse uses live-streaming and video-conferencing services in line with national and local safeguarding guidance / policies. Only tools within the Authorised Tech Stack may be used to deliver sessions. Where a session is recorded, transcribed or summarised (including by an AI note-taker), participants will be notified, such as via the Multiverse Privacy Notice. Recordings and transcripts will be stored in line with the Data Retention Policy.

15.2. In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children (under 18s) at Multiverse events for their own personal use (as such use is covered by the personal/household exemption under UK GDPR and the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published on networking sites or shared with anyone else, including via messaging groups.15.3. Learners must not take, record, screenshot, use, share, publish or distribute images of others without their permission.

15.4 Multiverse will only take and use images and recordings of learners where it has a lawful basis under UK GDPR. Where we rely on consent, for example for promotional use, it will be freely given, specific, informed, recorded and easy to withdraw. For learners under 18, we will consider whether the learner understands what they are agreeing to and can consent for themselves, and will involve a parent/carer where appropriate. Where we rely on another lawful basis, such as legitimate interests, we will assess the impact on the individual, with particular care for learners under 18, and respect their right to object. We will explain how images and recordings are used, where they are stored and how long they are kept, in our Privacy Notice and in line with the Data Retention Policy. Anyone can raise a concern or ask for an image to be removed by contacting the Data Protection Team at privacy@multiverse.io.

16. Data Protection

16.1 Multiverse processes personal data in connection with this policy, including filtering and monitoring logs, online safety and safeguarding records, and images and recordings. We do this in line with the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. We only collect what we need, keep it secure, share it only where the law allows (for example with the Safeguarding Team, the Internet Watch Foundation, NCA-CEOP or the police) and keep it no longer than necessary.

16.2 All Multiverse staff are required to complete data protection (GDPR) training during their induction and annually thereafter.

© Multiverse 2026

16.3 Our Privacy Notices explain what personal data we use, why, the lawful basis and how long we keep it. We will write them so that learners, including those under 18, can understand them.

16.4 New tools and processes that use personal data for online safety purposes, including AI tools, filtering and monitoring, moderation and recording, go through Multiverse's privacy review process before they are introduced. This looks at what data is used, why, the risks to individuals and how they will be managed, and results in a privacy assessment where one is needed. The Data Protection Officer is a member of the Online Safety Group, so privacy input is built into decisions about new tools.

16.5 Any personal data breach, or online safety incident involving personal data, must be reported immediately to the Data Protection Team at privacy@multiverse.io, and to the Safeguarding Team where there is a safeguarding concern (see section 9.9). Requests to exercise data protection rights should also go to the Data Protection Team.

17. Cyber Security

17.1. Multiverse has reviewed the DfE Cyber security standards and is working toward meeting these standards.

17.2. Multiverse conducts a cyber risk assessment annually.

17.3. Multiverse has an effective backup and restoration plan in place in the event of cyber attacks.

17.4. Multiverse's governance and IT policies reflect the importance of good cyber security.

17.5. Staff and Governors receive training on the common cyber security threats and incidents that Multiverse experience.

17.6. Multiverse has a business continuity and incident management plan in place for cyber security incidents.

17.7. There are processes in place for the reporting of cyber incidents. All learners and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this, and feel safe and comfortable to do so.

18. Community Hub and Moderation

All Multiverse learners are able to engage in an online forum and community environment, managed by Multiverse, called the Community Hub.

18.1. This online space is exclusive to Multiverse learners and alumni and is moderated manually, following the 'Multiverse Community Hub Moderation Guidelines and Escalation Procedure'.

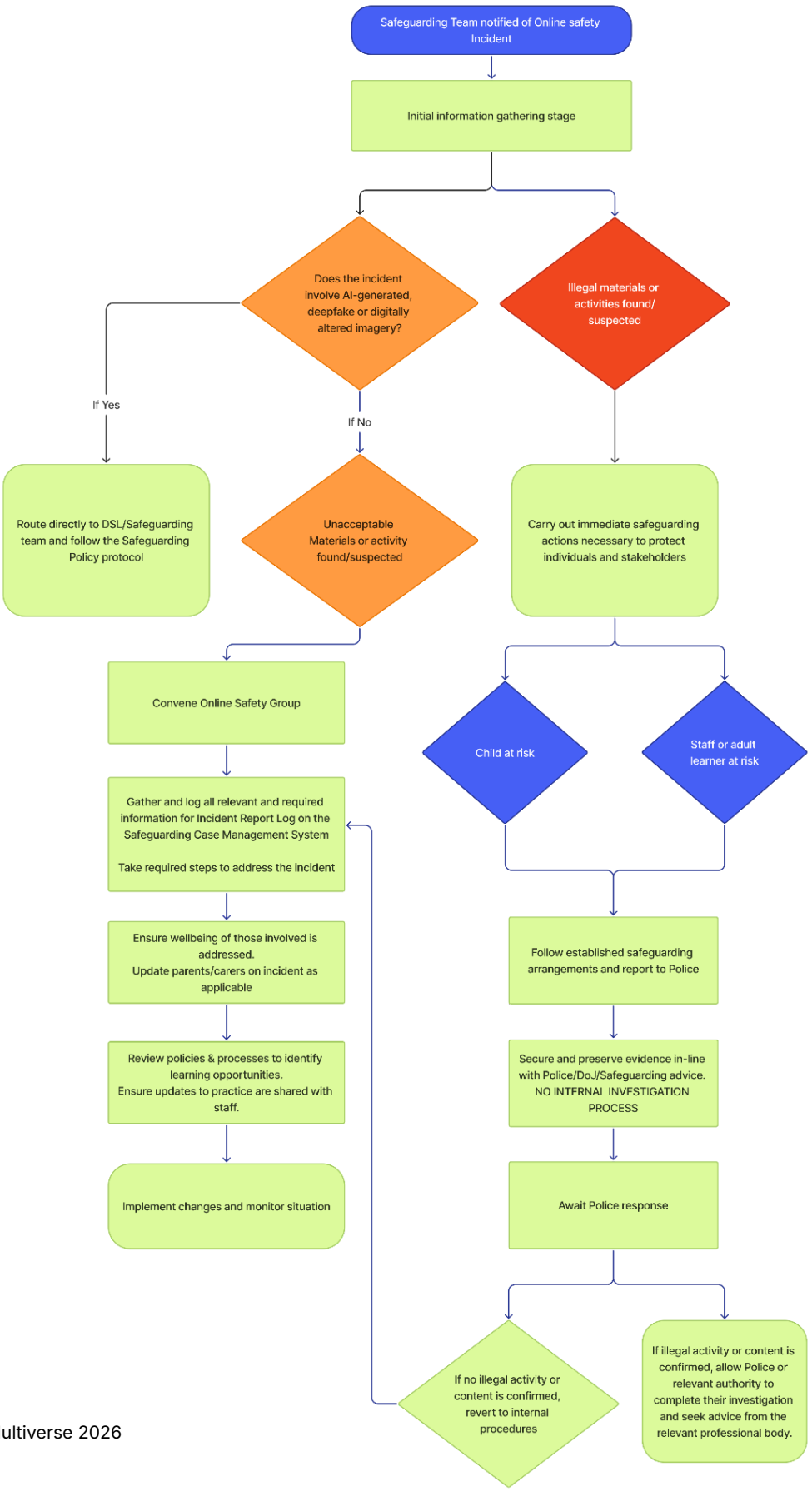
© Multiverse 2026

18.2. Incidents will be escalated to the Safeguarding Team, who subsequently will summarise these incidents and report them to the Online Safety Group.

18.3. The Online Safety Act 2023 and Ofcom's associated Children's Codes apply to user-to-user and search services that meet the Act's scope criteria. Education and childcare providers operating platforms for their own users are generally excluded from direct regulation under the Act. The Multiverse Community Hub is an internal platform exclusively for Multiverse learners and alumni, operated by Multiverse as an education provider for its own community. On this basis, the Community Hub is treated as out of scope of direct Ofcom regulation under the Act. Notwithstanding this position, Multiverse will continue to apply moderation standards consistent with Ofcom's Children's Codes as a voluntary benchmark of good practice, and will review this position in the event of any change to Ofcom's guidance on the scope of the Act or its application to further education and training providers.

© Multiverse 2026

Appendix One - Online Safety Incident Response Flow Chart 2026



© Multiverse 2026

Appendix Two

The following information should be recorded on the Safeguarding Case Management System if an Online Safety or Moderation Incident is reported, or flagged through filtering/monitoring:

1. Names and roles of staff conducting the review.
2. Name and role of the reporter.
3. Time and Date of incident.
4. Time and Date of review.
5. The form of incident e.g. Terrorism.
6. A description of the incident, including details such as the URL, or a screenshot if available.
7. Users involved in the incident.
8. Actions taken during the review, and by who.
9. Actions taken as a result of the review, and by who.
10. Confirmation that any screenshots have been deleted from personal devices and are now only stored on the Safeguarding Case Management System.
11. Whether the material may have been AI-generated, deep fake or digitally altered.
12. Whether the material was inadvertently viewed before being reported (and by whom).
13. Confirmation that DSL authorisation was obtained before any employer or third-party notification.
14. Whether the incident has been referred to external agencies (police, IWF, NCA-CEOP, local authority) and the dates of any referrals.

© Multiverse 2026