Online Safety Policy

Document Control:

Policy Owner	Designated Safeguarding Lead, Julia Bindley
Policy Author(s)	Safeguarding Implementation Lead, Jemma Ansell
Effective Date	*September 2025*
Version Number	[V1.0]
Date of Next Review	August 2026

Amendment History:

Version Number	Effective Date	Summary of Amendments	Author
[V1.0]			

1. Policy Introduction & Statement

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).

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.

3. Policy Development, Monitoring and Review

3.1. This Online Safety Policy has been developed by Multiverse's Online Safety Group made up of:

- The Designated Safeguarding Lead
- The Deputy Designated Safeguarding Lead
- Head of IT Operations

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	September 2026

annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	

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.

5. Roles and Responsibilities

5.1. CEO and Senior Leadership

- 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 Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The CEO and (at least) another member of the senior leadership team 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/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, Head of IT Operations 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/senior leaders 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/senior leaders will receive an annual report from the Online Safety Group.
- The CEO/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

5.2. Governors

- Governors are 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 Designated Safeguarding Lead / Online Safety Lead,
- 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 cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security 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
- 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/ Senior Leadership.
- 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.

5.4. The Deputy Designated Safeguarding Lead (DDSL)

- The DDSL leads the Online Safety Group.
- The DDSL works closely on a day-to-day basis with the Designated Safeguarding Lead (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 Keeping Children Safe in Education: 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, Keeping Children Safe in Education and UK GDPR regulations.
- 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 should only use Multiverse-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements.
- 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 and critically evaluated.

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
- The Deputy Designated Safeguarding Lead
- Head of IT Operations

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.
- Reviewing Community Hub moderation incident logs.
- Conducting an annual organisational Online Safety Risk Assessment/ 360-degree safe self review.
- Monitoring improvement actions identified through use of the risk assessment or self-review tool.

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.

7.1. The Online Safety Policy will be re-enforced through:

- Learner Flying Start.
- New employee contracts.
- Staff Multiverse 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 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					X

	• 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.					
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 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).					X
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	
	Access or share confidential information about Multiverse or any Multiverse Personnel or clients (except as authorised in the proper performance of duties).				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 Staff 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 received.
- The Designated Safeguarding Lead, Deputy Designated Safeguarding Lead 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.

8.2. 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.

8.3. 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.

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 guidance contained in Keeping Children Safe in Education and UK GDPR.

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

9.8. AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Data Protection Team. Quick reporting helps mitigate risks and facilitates a prompt response.

9.9. 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.

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

9.11. 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.

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.
- All Multiverse staff are mandated to complete GDPR UK Essentials Training and Cyber Security Awareness Training as part of their induction.
- Updates on online safety will be communicated internally to relevant staff through appropriate communication channels.
- The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead 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.

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.

11. Filtering and Monitoring

Multiverse has a statutory responsibility to ensure that appropriate filtering and monitoring systems are in place, as detailed in the Keeping Children Safe in Education guidance.

Multiverse's filtering and monitoring provision is agreed by senior leaders, governors and the Head of IT Operations 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 IT Operations. Individual concerns or incidents should be escalated by the Head of IT Operations to the Safeguarding Team as swiftly as possible. Overarching concerns with the suitability of the system should be raised by the Head of IT Operations to the Online Safety Group and senior leaders to be addressed.

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. A member of the senior leadership team and the Designated Safeguarding Lead, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.

Role	Responsibility
IT Operations	Ownership of all MV issued devices and authorised systems
WeWork	Network management for in office connections
Totality	MSP support of the IT ops team
Webroot	Web filtering and anti virus system

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., child sexual abuse images) 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. 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

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

11.1.6. Filtering logs are regularly reviewed by the Head of IT Operations, and results are brought to Online Safety Group on a quarterly basis, where the Designated Safeguarding Lead is informed of flagged incidents, and potential breaches to the Online Safety policy.

11.1.7. 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.

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

11.1.9. 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.

11.1.10. 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.

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 Designated Safeguarding Lead, 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 members of the senior leadership team and the Online Safety Group. The results of the review will be recorded and reported as relevant to the Quality Sub-Committee and Senior Leadership.

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

11.2.5. 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. Information Security Policy Guide

13. Mobile Technologies

The Devices and Acceptable Use Policy, alongside the Online Safety Policy details the expectations set by Multiverse around the use of mobile technologies. This covers both personal devices used on Multiverse networks and Multiverse-provided devices.

14. Social Media

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

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 not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on networking sites.

15.3. Learners must not take, use, share, publish or distribute images of others without their permission.

15.4. Photographs published on the Multiverse website, or elsewhere that include learners will be selected carefully and will comply with the following principles. The full names and workplaces of any learners under 18 will not be used anywhere on a website or post, particularly in association with photographs, and consent from parents/carers will be obtained before photographs of learners under 18 are taken. Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long.

16. Data Protection

A clear Data Security Policy and Data Retention Policy stipulates how personal data will be recorded, processed, transferred and made available, according to the current data protection legislation.

17. Cyber Security

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

18.2. Multiverse conducts a cyber risk assessment annually.

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

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

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

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

18.7. 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.

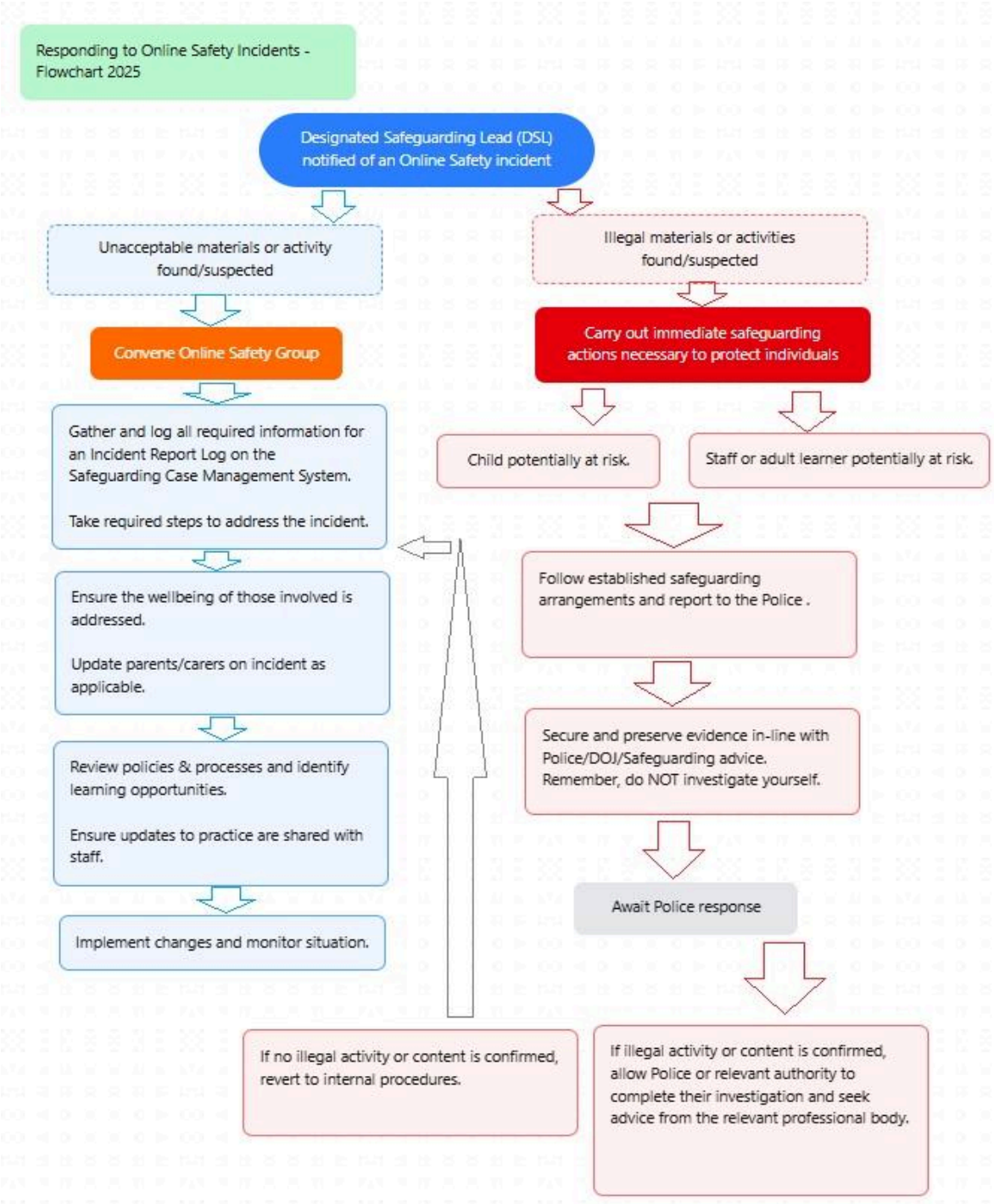
18. Community Hub and Moderation

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 Multiverse alumni and is moderated manually, following the ‘Multiverse Community Hub Moderation Guidelines and Escalation Procedure.’

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

Appendix One - Online Safety Incident Response Flow Chart 2025



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.