



Online Safety Policy

Approved by: Board of Directors

Policy Owner: Storyy Education

Responsible Senior Lead: Natalie Lee

Date Approved: August 2026

Review Cycle: Annually and as required

Next Review Date: August 2027

Version: 2.0

Contents

1. Policy Statement	3
2. Vision and Purpose.....	3
3. Legislative and Regulatory Framework	4
4. Storyy Education as an Alternative Provision Provider	5
5. Digital Safeguarding Principles.....	6
6. Online Safety Curriculum	7
7. Safeguarding Through Technology	8
8. Artificial Intelligence (AI) and Emerging Technologies.....	9
9. Acceptable Use of Digital Technology	10
9.3 Student Acceptable Use	12
10. Mobile Phones, Smart Devices and Social Media	13
11. Reporting Concerns and Responding to Online Safety Incidents.....	15
12. Roles and Responsibilities	16
13. Monitoring, Evaluation and Quality Assurance	17
14. Links with Other Policies.....	17
15. Filtering, Monitoring and Cyber Security	18
Appendix A – Digital Safety Curriculum Framework	19
Appendix B – Online Risks Progression.....	20
Appendix C – AI Decision Tree ("Can I use AI for this?")	21
Appendix D – Online Safety Incident Flowchart.....	22
Appendix E – Filtering & Monitoring Escalation Process	23

1. Policy Statement

Storyy Education is committed to creating safe, supportive and inclusive learning environments where every student can benefit from digital technology whilst being protected from harm. The organisation recognises that technology plays an integral role in modern education, communication and everyday life, providing significant opportunities for learning, creativity, collaboration and preparation for adulthood. At the same time, digital technologies present safeguarding risks that require a proactive, informed and whole-organisation approach.

As a specialist Alternative Provision provider delivering the RESET and BRIGHT programmes, Storyy Education works with many young people who have experienced disrupted education, trauma, adverse childhood experiences, emotionally based school avoidance (EBSA), unmet special educational needs and disabilities (SEND), social, emotional and mental health (SEMH) needs or other vulnerabilities. These experiences may increase a student's exposure to online harm or reduce their confidence in recognising and responding to digital risks. Storyy Education therefore regards online safety as a fundamental safeguarding responsibility rather than simply an aspect of information technology.

Online safety is embedded throughout the wider curriculum, therapeutic mentoring, restorative practice and everyday interactions with students. Through planned teaching, positive relationships and practical experiences, students develop the knowledge, skills and confidence needed to use technology safely, responsibly and respectfully, whilst recognising risks, protecting themselves and others and making informed decisions in an increasingly digital world.

This policy establishes Storyy Education's approach to online safety, digital safeguarding and the acceptable use of technology by students, staff, volunteers, contractors and visitors. It reflects the organisation's commitment to safeguarding, promoting positive digital citizenship and maintaining secure digital systems that support high-quality education and effective professional practice.

The policy should be read alongside the Storyy Education Child Protection and Safeguarding Policy, Positive Behaviour, Relationships and Emotional Regulation Policy, PSHE and RSHE Policy, Curriculum Policy, Attendance Policy, Mobile Phone and Smart Device Policy, Equality, Diversity and Inclusion Policy, Data Protection Policy and Staff Code of Conduct to ensure a consistent and coordinated approach across the organisation.

2. Vision and Purpose

Storyy Education believes that every young person should be equipped with the knowledge, understanding and confidence needed to participate safely, responsibly and successfully within the digital world. Technology should enhance learning, strengthen communication, increase opportunities and prepare students for adult life whilst never compromising their safety, wellbeing or dignity.

The organisation recognises that online safety is not achieved solely through filtering systems or restricting access to technology. Effective digital safeguarding is achieved through education, trusted relationships, professional curiosity and the development of critical thinking, enabling students to recognise risk, make informed decisions and seek support whenever concerns arise.

Many students referred to Storyy Education have experienced interrupted education or inconsistent access to high-quality online safety education. As a result, some students may require additional support to develop digital resilience, recognise manipulation or exploitation, understand healthy online relationships or safely navigate emerging technologies such as artificial intelligence. Storyy

'We're creating a world where every young person has a brighter future'

Education therefore delivers online safety through a stage-not-age, trauma-informed approach that reflects each student's developmental stage, previous experiences and individual needs.

The Online Safety, Digital Technology and Acceptable Use Policy aims to:

- safeguard students from online harm, abuse and exploitation;
- promote responsible, respectful and ethical use of digital technology;
- develop confident and informed digital citizens;
- support staff to model safe and professional online behaviour;
- establish clear expectations for the acceptable use of technology;
- ensure that digital safeguarding remains fully integrated within the organisation's wider safeguarding arrangements;
- prepare students for safe participation in education, employment and modern society.

Through RESET and BRIGHT, Storyy Education seeks not only to keep students safe today but to equip them with the lifelong digital skills, judgement and resilience needed to thrive in an increasingly connected world.

3. Legislative and Regulatory Framework

Storyy Education is committed to maintaining the highest standards of online safety and digital safeguarding. This policy has been developed with reference to current legislation, statutory guidance and recognised best practice, ensuring that the organisation's arrangements remain consistent with national safeguarding expectations and the responsibilities of Alternative Provision providers.

This policy should be read alongside the latest versions of:

- Keeping Children Safe in Education (KCSIE) 2026;
- Working Together to Safeguard Children;
- The Online Safety Act 2023;
- Education for a Connected World Framework;
- Teaching Online Safety in Schools;
- The Prevent Duty Guidance;
- The UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Equality Act 2010;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- SEND Code of Practice: 0–25 Years;
- Alternative Provision Statutory Guidance;

‘We’re creating a world where every young person has a brighter future’

- DfE Filtering and Monitoring Standards for Schools and Colleges;
- ICO guidance relating to children's data, privacy and information security.

Storyy Education recognises that online safety is inseparable from safeguarding. Digital technologies can present opportunities for learning whilst also exposing children and young people to abuse, exploitation, bullying, harmful content, criminal activity, misinformation and emerging risks associated with artificial intelligence and rapidly developing online platforms. Consequently, online safety is embedded throughout safeguarding practice, curriculum delivery and organisational decision-making.

The organisation will review this policy regularly to reflect legislative changes, technological developments, emerging safeguarding risks and updated national guidance, ensuring that practice remains current, effective and responsive.

4. Storyy Education as an Alternative Provision Provider

Storyy Education is a specialist Alternative Provision provider delivering the RESET and BRIGHT programmes to children and young people experiencing barriers to education, including disrupted learning, trauma, exclusion, emotionally based school avoidance (EBSA), SEND, SEMH needs, medical needs and other vulnerabilities affecting successful participation in education.

Storyy Education is not a registered school and does not replace the statutory safeguarding, curriculum or governance responsibilities of a student's commissioning school or local authority unless these responsibilities have been formally delegated through contractual arrangements.

Digital safeguarding is therefore a shared responsibility between Storyy Education, commissioning schools, local authorities, parents or carers and other relevant professionals. Storyy Education works collaboratively with commissioning partners to ensure that online safety education, safeguarding arrangements and acceptable use expectations are consistent, coordinated and responsive to each student's individual circumstances.

Online learning and digital technology may be used across a wide range of Storyy Education environments, including RESET Primary, RESET Secondary, BRIGHT Outreach, home-based learning, community settings, vocational placements, educational visits and remote engagement. Staff ensure that appropriate safeguarding arrangements, supervision and risk assessments are in place regardless of where digital learning takes place.

Before digital learning activities are planned, staff consider the student's developmental stage, previous online safety education, SEND needs, EHCP outcomes, safeguarding history, emotional wellbeing, access to technology, parental support and any known contextual safeguarding risks. This ensures that learning remains personalised, proportionate and appropriate whilst maintaining high expectations for every student.

Storyy Education also recognises that many students may have experienced inconsistent supervision online, unrestricted access to digital platforms or previous exposure to harmful online experiences. The organisation therefore places a strong emphasis on rebuilding digital confidence, promoting healthy online behaviours and teaching practical strategies that enable students to recognise risk, seek support and participate safely within an increasingly connected world.

5. Digital Safeguarding Principles

Digital safeguarding is embedded throughout every aspect of Storyy Education's practice and forms an integral part of the organisation's wider safeguarding culture. The use of technology should enhance learning, communication, creativity and personal development whilst ensuring that students, staff and the wider community remain safe, respected and protected from harm. Online safety is therefore considered within all aspects of curriculum planning, mentoring, safeguarding, behaviour support and daily practice.

The following principles underpin the delivery of online safety, digital technology and acceptable use throughout Storyy Education.

5.1 Safeguarding First

The safety and wellbeing of children and young people will always take priority over the use of technology. Decisions relating to digital learning, internet access, online platforms, artificial intelligence and communication technologies will always be informed by safeguarding considerations and individual risk assessments where appropriate. Staff understand that online safety is a safeguarding responsibility and will respond to concerns in accordance with the Storyy Education Child Protection and Safeguarding Policy.

5.2 Education Before Restriction

Whilst appropriate filtering, monitoring and security systems are essential, Storyy Education recognises that technology alone cannot keep young people safe. Students are therefore taught how to recognise online risks, think critically, make informed decisions and seek help when concerns arise. The organisation aims to develop confident, resilient and responsible digital citizens who can apply these skills beyond their time at Storyy Education.

5.3 Stage-not-Age Learning

Online safety education is delivered using Storyy Education's stage-not-age approach. Staff recognise that many students have experienced disrupted education, inconsistent curriculum coverage or gaps in previous learning. Digital safety education is therefore planned according to each student's developmental stage, understanding, previous experiences and identified needs whilst maintaining age-appropriate expectations and respectful learning environments.

5.4 Trauma-Informed Practice

Many students accessing RESET and BRIGHT have experienced trauma, adverse childhood experiences, emotionally based school avoidance (EBSA), exploitation or other significant vulnerabilities. Staff recognise that these experiences may influence how students use technology, form online relationships, respond to digital communication or engage with online content. Online safety education is therefore delivered through positive relationships, emotional safety, restorative practice and predictable routines that support confidence, trust and resilience.

5.5 Inclusion and Accessibility

Storyy Education is committed to ensuring that every student can access online safety education regardless of their individual needs. Teaching is adapted appropriately for students with SEND, including Autism Spectrum Condition (ASC), Attention Deficit Hyperactivity Disorder (ADHD), Social, Emotional and Mental Health (SEMH) needs, Speech, Language and Communication Needs (SLCN),

cognition and learning difficulties, sensory needs and physical disabilities. Reasonable adjustments are made where necessary to ensure that learning remains ambitious, accessible and meaningful.

5.6 Positive Digital Citizenship

Storyy Education promotes responsible, respectful and ethical use of technology. Students are encouraged to consider how their online behaviour affects themselves and others, understand their digital footprint, respect privacy, challenge discrimination, communicate appropriately and contribute positively to online communities. Staff model professional and responsible digital behaviour at all times, recognising that children and young people learn through observation as well as direct teaching.

5.7 Shared Responsibility

Maintaining online safety is a shared responsibility between Storyy Education, students, parents or carers, commissioning schools, local authorities and partner agencies. Effective communication, information sharing and collaborative working ensure that online safety messages remain consistent across all environments in which students access education and technology. Storyy Education works proactively with families and commissioning partners to support safe, responsible and appropriate use of digital technology both within and beyond the provision.

5.8 Preparing Students for Modern Digital Life

Technology continues to evolve rapidly, creating new opportunities alongside emerging safeguarding risks. Storyy Education aims to prepare students not only for their current educational experiences but also for successful participation in further education, employment and adult life. This includes developing digital literacy, critical thinking, responsible use of artificial intelligence, cyber awareness, online professionalism and the confidence to navigate future technologies safely and responsibly.

6. Online Safety Curriculum

Storyy Education recognises that online safety cannot be taught through isolated lessons alone. Instead, digital safeguarding is embedded throughout the wider curriculum, PSHE and RSHE, therapeutic mentoring, restorative conversations, enrichment activities and everyday interactions with trusted adults. Learning is progressive, responsive to individual need and closely linked to each student's wider personal development, safeguarding needs and preparation for adulthood.

The online safety curriculum complements the student's commissioned provision and is delivered through the RESET and BRIGHT programmes using practical, discussion-based and real-life learning experiences. Curriculum content is reviewed regularly to reflect emerging technologies, changing online behaviours, national safeguarding priorities and the individual circumstances of students.

The curriculum is organised around six key strands.

6.1 Healthy Digital Relationships

Students develop the knowledge and skills required to build respectful, safe and healthy relationships within digital environments. Teaching explores appropriate online communication, respect for others, consent, personal boundaries, cyberbullying, peer pressure, positive behaviour on social media and the importance of recognising unhealthy or abusive online relationships.

6.2 Keeping Safe Online

Students are supported to recognise online risks and develop practical strategies to protect themselves and others. Learning includes online privacy, passwords, personal information, scams, phishing, identity theft, grooming, exploitation, inappropriate contact, location sharing and recognising situations that require adult support or safeguarding intervention.

6.3 Digital Citizenship

The curriculum promotes responsible participation within online communities by encouraging students to consider the impact of their digital behaviour, online reputation and digital footprint. Students develop an understanding of respect, copyright, intellectual property, responsible sharing of information and the long-term consequences of online activity.

6.4 Critical Thinking and Artificial Intelligence

Students develop the ability to evaluate online information critically and make informed decisions about digital content. Teaching includes misinformation, disinformation, fake news, manipulated media, online influencers, advertising, algorithms and the responsible use of artificial intelligence. Students are encouraged to question the reliability of online information and understand that AI-generated content should always be verified before being accepted as accurate.

6.5 Digital Health and Wellbeing

Storyy Education promotes healthy and balanced use of technology. Students explore topics including screen time, gaming, social media, emotional wellbeing, healthy routines, sleep, online behaviour, digital addiction and maintaining positive relationships both online and offline. Teaching encourages students to recognise when technology supports wellbeing and when it may become harmful or overwhelming.

6.6 Preparing for Adult Digital Life

As students progress through RESET and BRIGHT, increasing emphasis is placed upon developing the digital knowledge and skills required for further education, employment and independent living. Learning includes professional online conduct, digital communication, online banking awareness, financial scams, cyber security, employability, responsible use of workplace technology and maintaining a positive digital reputation.

7. Safeguarding Through Technology

Online safety is an integral part of Storyy Education's safeguarding arrangements and is embedded throughout the organisation's culture, curriculum and daily practice. Staff recognise that digital technology can enhance learning, communication and personal development whilst also exposing children and young people to significant safeguarding risks. Storyy Education therefore adopts a proactive and preventative approach that combines education, trusted relationships, professional curiosity and effective safeguarding procedures.

Many students accessing RESET and BRIGHT have experienced disrupted education, trauma, exploitation, emotionally based school avoidance (EBSA), unmet SEND needs or social, emotional and mental health (SEMH) difficulties that may increase their vulnerability online. Staff understand that these factors may affect how students engage with technology, form online relationships or respond to digital communication. Online safeguarding is therefore personalised and responsive to

each student's individual circumstances, recognising that risks may differ significantly between students.

Through the online safety curriculum, mentoring, restorative conversations and everyday interactions, students are supported to recognise online risks, develop protective behaviours and understand how to seek help if something online makes them feel worried, uncomfortable or unsafe. Particular emphasis is placed on developing confidence to report concerns, recognising that many young people experiencing online abuse may feel embarrassed, frightened or uncertain about asking for support.

Storyy Education teaches students about a broad range of online safeguarding risks appropriate to their age, stage of development and individual needs. These include online grooming, child sexual exploitation, child criminal exploitation, county lines, radicalisation and extremism, cyberbullying, child-on-child abuse, harmful sexual behaviour, online coercion, sextortion, sharing of indecent images, inappropriate online relationships, online fraud, financial scams, misinformation, disinformation, artificial intelligence, exposure to harmful or illegal content and the misuse of social media, gaming platforms and digital communication.

The organisation also recognises the increasing risks associated with anonymous messaging applications, livestreaming, location sharing, online influencers, image manipulation, deepfakes and AI-generated content. Students are encouraged to think critically about the information they encounter online, question the reliability of digital content and understand that not everything they see or read online is accurate, safe or trustworthy.

Where concerns arise, staff respond in accordance with the Storyy Education Child Protection and Safeguarding Policy. Online safety concerns are treated as safeguarding concerns whenever there is reason to believe that a student may be at risk of abuse, neglect, exploitation or significant harm. Staff will listen carefully, respond appropriately, avoid judgement and follow the organisation's safeguarding procedures without delay.

Any online safeguarding concern, disclosure or incident will be recorded promptly and factually within CPOMS and referred immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL. The DSL will determine appropriate next steps, including liaison with parents or carers where appropriate, commissioning schools, local authorities, children's social care, the Police, CEOP or other relevant agencies in accordance with statutory safeguarding guidance.

Storyy Education recognises that safeguarding through technology extends beyond responding to incidents. Staff remain professionally curious, monitor emerging safeguarding themes, maintain up-to-date knowledge of evolving digital risks and receive regular safeguarding and online safety training. Lessons learned from incidents, national guidance and local safeguarding intelligence inform ongoing curriculum development, staff training and organisational practice.

By embedding online safety throughout the wider safeguarding culture, Storyy Education seeks not only to protect students from immediate harm but also to equip them with the resilience, judgement and confidence required to participate safely within an increasingly connected digital world.

8. Artificial Intelligence (AI) and Emerging Technologies

Storyy Education recognises that artificial intelligence (AI) is becoming an increasingly significant part of education, employment and everyday life. AI technologies have the potential to enhance learning,

'We're creating a world where every young person has a brighter future'

creativity, accessibility and productivity, whilst also presenting new safeguarding, ethical and educational challenges. The organisation is committed to ensuring that both staff and students understand how AI can be used safely, responsibly and appropriately.

Artificial intelligence may be used within Storyy Education to support learning, curriculum planning, administrative processes and the development of personalised educational resources. However, AI must never replace professional judgement, safeguarding responsibilities or meaningful relationships between staff and students. All information generated through AI should be critically evaluated, verified against reliable sources where appropriate and used in a manner that supports rather than undermines learning.

Students are taught that AI-generated content may be inaccurate, misleading, biased or entirely fabricated. Through the online safety and wider curriculum, they develop the critical thinking skills required to question information, recognise the limitations of AI and understand the importance of verifying digital content before relying upon it. They are also supported to understand issues relating to copyright, plagiarism, academic integrity, privacy and the ethical use of emerging technologies.

Staff using AI remain responsible for the accuracy, quality and appropriateness of any material produced. Confidential, personal or safeguarding information must never be entered into publicly available AI platforms unless this is authorised, compliant with data protection legislation and approved through Storyy Education's information governance arrangements. Professional judgement must always take precedence over AI-generated suggestions or recommendations.

Artificial intelligence must not be used to generate behaviour records, safeguarding decisions, risk assessments or professional opinions without appropriate review by a suitably qualified member of staff. Decisions affecting students will always remain the responsibility of Storyy Education professionals and will be informed by direct knowledge of the student, professional expertise and organisational safeguarding procedures.

As technology continues to evolve, Storyy Education will regularly review its approach to artificial intelligence, ensuring that emerging opportunities and risks are reflected within staff training, curriculum planning and safeguarding arrangements. The organisation is committed to promoting responsible innovation whilst maintaining the highest standards of safeguarding, privacy, educational integrity and professional accountability.

9. Acceptable Use of Digital Technology

Storyy Education recognises that digital technology is essential for learning, communication, safeguarding and the effective operation of the organisation. All users of Storyy Education technology are expected to use digital systems responsibly, professionally and lawfully, ensuring that their actions support safeguarding, protect confidential information and promote a positive learning environment.

The expectations within this section apply to all staff, volunteers, students, contractors, visitors and any individual accessing Storyy Education's digital systems, devices or network services.

9.1 General Expectations

Everyone using technology within Storyy Education is expected to use digital resources safely, respectfully and responsibly. Technology should only be used for legitimate educational, safeguarding or organisational purposes and in ways that reflect the values of the organisation.

'We're creating a world where every young person has a brighter future'

Users are expected to:

- protect their own accounts, passwords and authentication credentials;
- respect the privacy and dignity of others;
- access only information that they are authorised to view;
- report any concerns relating to online safety, cyber security or inappropriate digital content immediately;
- comply with all safeguarding, confidentiality and data protection requirements;
- use digital technology in a manner that supports learning, wellbeing and positive relationships.

Any misuse of technology may result in disciplinary procedures, safeguarding action, withdrawal of access or referral to external agencies where appropriate.

9.2 Staff Acceptable Use

Staff play a vital role in modelling safe, professional and responsible use of technology. All staff are expected to maintain the highest standards of professional conduct whenever using digital devices, online platforms or electronic communication.

Staff must:

- use Storyy Education devices and systems primarily for professional purposes;
- maintain secure passwords and protect access to organisational systems;
- immediately report suspected cyber security incidents or data breaches;
- ensure confidential information is stored, shared and disposed of securely;
- use only authorised software, applications and digital platforms;
- maintain appropriate professional boundaries when communicating electronically with students;
- follow the organisation's policies regarding mobile phones, photography, social media and artificial intelligence;
- ensure that any safeguarding concerns identified through technology are recorded promptly on CPOMS and reported to the Designated Safeguarding Lead.

Staff must not:

- share passwords or login credentials;
- access inappropriate, offensive or illegal material;
- install unauthorised software;
- use personal email accounts for organisational business;
- communicate with students through personal social media accounts or unauthorised messaging platforms;

'We're creating a world where every young person has a brighter future'

- record, photograph or film students using personal devices unless specifically authorised in exceptional circumstances and in accordance with organisational procedures;
- enter confidential student information into publicly available AI platforms.

Professional judgement, safeguarding responsibilities and confidentiality must always take precedence over convenience when using technology.

9.3 Student Acceptable Use

Storyy Education encourages students to use technology positively and responsibly as part of their education and preparation for adulthood. Students are expected to demonstrate respect for themselves and others whenever using digital technology, whether within Storyy Education or elsewhere.

Students are expected to:

- use technology safely and respectfully;
- follow staff instructions regarding digital devices;
- protect their own passwords and personal information;
- report anything online that makes them feel worried, uncomfortable or unsafe;
- respect the privacy of others;
- use technology to support learning and personal development.

Students must not:

- deliberately access inappropriate or illegal content;
- use technology to bully, threaten, intimidate or harass others;
- photograph, film or record another person without permission;
- share personal information that may place themselves or others at risk;
- attempt to bypass security, filtering or monitoring systems;
- deliberately damage or misuse Storyy Education equipment or digital services.

Where inappropriate use occurs, staff will respond using education, restorative practice and safeguarding procedures alongside any necessary behaviour management measures.

9.4 Personal Devices

Storyy Education recognises that mobile phones, tablets and other personal devices form an important part of modern life. However, their use within the provision must never compromise safeguarding, learning, confidentiality or the wellbeing of others.

The use of personal devices by staff and students is governed by the Storyy Education Mobile Phone and Smart Device Policy. Any photography, filming, audio recording or live streaming must be authorised and comply with safeguarding requirements, data protection legislation and parental consent arrangements.

9.5 Internet, Email and Network Use

Access to the internet is provided to support education, safeguarding and organisational business. Storyy Education operates appropriate filtering, monitoring and cyber security arrangements to reduce exposure to harmful or illegal material whilst recognising that no filtering system can completely eliminate online risk.

Users are expected to use email, internet services, cloud storage and digital communication professionally, responsibly and in accordance with organisational procedures. Any attempt to access inappropriate material, circumvent security measures, introduce malicious software or misuse organisational systems may result in disciplinary action and, where appropriate, referral to external agencies.

9.6 Data Protection and Information Security

Everyone using Storyy Education technology shares responsibility for protecting personal information and maintaining information security. Confidential information must only be accessed by authorised individuals and handled in accordance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018** and Storyy Education's Data Protection Policy.

Personal information relating to students, families, staff or partner organisations must be stored securely, shared only where lawful and necessary, and protected from unauthorised access, accidental loss or inappropriate disclosure.

9.7 Monitoring and Compliance

To protect students, staff and organisational systems, Storyy Education reserves the right to monitor the use of its digital networks, devices, internet services and communication systems where lawful and proportionate to do so. Monitoring is undertaken to support safeguarding, maintain cyber security, investigate concerns, ensure compliance with organisational policies and protect the integrity of the organisation's systems.

Users should not expect complete privacy when using Storyy Education equipment or digital services. Monitoring will always be undertaken in accordance with data protection legislation, employment law and organisational procedures, ensuring that it remains proportionate, transparent and respectful of individual rights.

10. Mobile Phones, Smart Devices and Social Media

Digital technology, including mobile phones, smart watches, tablets and other internet-enabled devices, plays an increasingly important role in education and everyday life. Storyy Education recognises that these technologies can support communication, learning and independence whilst also presenting safeguarding, privacy and wellbeing risks. Clear expectations are therefore established to ensure that technology is used safely, responsibly and appropriately.

10.1 Student Mobile Phones and Personal Devices

Storyy Education expects students to use personal technology responsibly and in accordance with staff instructions. Mobile phones and other personal devices must not disrupt learning, compromise safeguarding or infringe upon the privacy of others.

The arrangements for student mobile phone use may vary according to the individual student, programme, activity, risk assessment or placement objectives. Where appropriate, students may be

asked to hand mobile phones or other devices to a member of staff at the beginning of a session or store them securely until required. This approach supports concentration, promotes positive engagement and reduces unnecessary distractions whilst remaining sensitive to individual circumstances.

Students must not use personal devices to photograph, film or record staff, students or visitors without explicit permission. The unauthorised sharing of images, videos, audio recordings or personal information is strictly prohibited and will be managed in accordance with the Behaviour Policy and Child Protection and Safeguarding Policy.

Where a student uses technology in a manner that presents a safeguarding concern, staff will prioritise safety, respond proportionately and follow the organisation's safeguarding procedures. Responses will focus on education, restorative practice and positive behaviour support wherever possible.

10.2 Staff Mobile Phones and Personal Devices

Staff are expected to model safe, responsible and professional use of technology at all times. Personal mobile phones should not distract from supervision, teaching, mentoring or safeguarding responsibilities and should only be used during working hours where appropriate and in accordance with organisational procedures.

Personal devices must never be used to photograph, film or record students except in exceptional circumstances where no suitable organisational device is available, the action is authorised by the Provision Manager and any images are transferred securely to Storyy Education systems before being deleted immediately from the personal device.

Staff must not communicate with students through personal social media accounts, personal messaging applications or private telephone numbers unless specifically authorised as part of an agreed organisational communication process. Professional boundaries must always be maintained.

10.3 Smart Devices and Wearable Technology

The increasing use of smart watches, fitness trackers, voice assistants and other connected devices presents additional safeguarding and privacy considerations. Storyy Education may restrict the use of wearable technology where it interferes with learning, compromises safeguarding, enables unauthorised communication or creates unnecessary distractions.

Where wearable devices include cameras, microphones, internet access or communication functions, staff may require them to be removed or switched off during learning activities.

10.4 Photography, Filming and Digital Media

Photography, filming and audio recording must always respect the dignity, privacy and safety of every individual. Images or recordings of students may only be taken using authorised Storyy Education equipment and in accordance with parental consent, data protection legislation and the organisation's media procedures.

Students, visitors and members of the public are not permitted to photograph or film other individuals without permission. Any misuse of digital media that compromises safeguarding, confidentiality or privacy will be treated seriously and managed through the appropriate safeguarding and behaviour procedures.

10.5 Social Media

Storyy Education recognises that social media forms an important part of many young people's lives and provides opportunities for communication, creativity and learning. However, social media also presents safeguarding risks including cyberbullying, grooming, exploitation, misinformation, inappropriate contact, reputational harm and breaches of privacy.

Students are encouraged to think critically about the content they view and share online, understand the permanence of their digital footprint and use social media respectfully and responsibly. Staff reinforce these messages through the wider curriculum, mentoring and restorative conversations.

Staff must maintain professional boundaries at all times and must not accept friend requests, follow students through personal accounts or engage with students using private social networking platforms. Organisational social media accounts must only be managed by authorised staff in accordance with Storyy Education's communication procedures.

10.6 Responding to Concerns

Any concerns relating to mobile phones, personal devices, social media or digital communication that indicate a safeguarding risk will be managed in accordance with the Storyy Education Child Protection and Safeguarding Policy. Staff will respond promptly, preserve evidence where appropriate, record concerns on CPOMS and report them immediately to the Designated Safeguarding Lead (DSL).

Where concerns involve criminal activity, exploitation, indecent images of children, online coercion, threats or other serious offences, Storyy Education will work with commissioning schools, local authorities, the Police, CEOP and other relevant agencies as appropriate.

11. Reporting Concerns and Responding to Online Safety Incidents

Storyy Education encourages all students, staff, parents, carers and visitors to report any online safety concern, cyber security issue or inappropriate use of technology without delay. Concerns will always be taken seriously and responded to promptly, proportionately and in accordance with the organisation's safeguarding procedures.

Online safety concerns may arise in a variety of ways, including disclosures from students, observations by staff, filtering or monitoring systems, reports from parents or carers, information received from commissioning schools or partner agencies, or concerns identified through mentoring, restorative conversations or wider safeguarding practice. Regardless of how concerns are identified, the safety and wellbeing of the student will remain the primary consideration.

Where an online safety concern presents, or may present, a safeguarding risk, staff must respond in line with the Child Protection and Safeguarding Policy. Concerns should be recorded factually and without delay on CPOMS before being reported immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL. Staff should never investigate safeguarding concerns independently or attempt to manage serious incidents without appropriate support.

The DSL will assess the concern, determine any immediate protective actions required and coordinate appropriate referrals or information sharing with parents or carers, commissioning schools, local authorities, children's social care, the Police, CEOP or other relevant agencies where

necessary. Responses will always be proportionate to the level of risk and guided by statutory safeguarding responsibilities.

Where incidents do not meet safeguarding thresholds but indicate inappropriate use of technology, staff will respond through education, restorative practice, behaviour support and digital safety education. Wherever possible, incidents will be used as opportunities to strengthen students' understanding of safe, responsible and respectful use of technology.

Following any significant online safety incident, Storyy Education will review the circumstances, identify any lessons learned and consider whether updates are required to individual risk assessments, behaviour support plans, curriculum delivery, staff training or organisational procedures. This process supports continuous improvement and helps ensure that safeguarding arrangements remain responsive to emerging technologies and evolving online risks.

12. Roles and Responsibilities

Promoting online safety is a shared responsibility across Storyy Education. Every member of the organisation has a role in creating a safe digital environment, modelling responsible use of technology and protecting students from online harm.

The **Board of Directors** is responsible for ensuring that appropriate governance arrangements are in place to support effective online safety, digital safeguarding and information security across the organisation. The Board monitors compliance with statutory guidance, approves organisational policies and ensures that sufficient resources are available to maintain safe digital systems and effective staff training.

The **Managing Director** provides strategic leadership for online safety and digital safeguarding, ensuring that this policy is implemented consistently across Storyy Education. The Managing Director is responsible for ensuring that digital safeguarding remains aligned with current legislation, organisational policies and the wider safeguarding framework.

The **Designated Safeguarding Lead (DSL)** has strategic responsibility for overseeing online safeguarding concerns, monitoring emerging digital risks and ensuring that staff respond appropriately to technology-facilitated safeguarding issues. The DSL manages referrals, oversees safeguarding records held on **CPOMS**, coordinates multi-agency working where required and ensures that online safety remains embedded within safeguarding practice.

Provision Managers are responsible for the day-to-day implementation of this policy within their provision. They ensure that staff understand their responsibilities, appropriate digital safeguarding measures are maintained, curriculum delivery reflects current online safety risks and concerns are managed consistently and effectively.

Mentors, Tutors and all Staff are responsible for modelling safe and professional use of technology, delivering online safety education, maintaining appropriate professional boundaries, identifying safeguarding concerns and following organisational procedures for recording and reporting concerns. Staff are expected to maintain professional curiosity and remain informed about emerging online risks affecting children and young people.

Parents and Carers are recognised as important partners in promoting safe technology use. Storyy Education encourages open communication with families, sharing appropriate guidance and working collaboratively to support students in developing safe, responsible and respectful digital behaviours both within and beyond the provision.

'We're creating a world where every young person has a brighter future'

Students are encouraged to use technology safely, responsibly and respectfully, follow staff guidance, report concerns promptly and contribute positively to maintaining a safe digital learning environment. Through the RESET and BRIGHT programmes, students are supported to become increasingly independent, responsible and resilient digital citizens.

Commissioning Schools and Local Authorities retain responsibility for the student's wider statutory safeguarding and educational arrangements where applicable. Storyy Education works collaboratively with commissioners to share relevant information, coordinate safeguarding responses and ensure that online safety education complements the student's broader curriculum and support arrangements.

13. Monitoring, Evaluation and Quality Assurance

Storyy Education is committed to continually improving its approach to online safety, digital safeguarding and acceptable use of technology. Regular monitoring and evaluation ensure that this policy remains effective, reflects current legislation and responds to emerging technologies and safeguarding risks.

Senior leaders and Provision Managers monitor the implementation of this policy through quality assurance activities, curriculum review, safeguarding oversight and professional supervision. Monitoring considers the effectiveness of online safety education, the consistency of staff practice and the organisation's ability to identify and respond to emerging digital safeguarding concerns.

Quality assurance includes reviewing curriculum coverage, staff training, student voice, digital safeguarding incidents, behaviour trends, attendance, intervention outcomes, online safety concerns recorded within CPOMS, feedback from parents and carers, commissioner feedback and developments within national safeguarding guidance. Information gathered through these processes informs curriculum development, staff training, organisational improvement and policy review.

Filtering and monitoring arrangements are reviewed regularly to ensure that they remain appropriate to the organisation's digital environment and continue to support safeguarding without unnecessarily restricting learning opportunities. Lessons learned from incidents, safeguarding reviews or changes in technology are used to strengthen practice across Storyy Education.

This policy will be reviewed at least annually, or sooner where significant changes in legislation, statutory guidance, technology or organisational practice require amendment. Through a culture of reflection and continuous improvement, Storyy Education seeks to maintain the highest standards of digital safeguarding and prepare students to participate safely and confidently within an increasingly connected world.

14. Links with Other Policies

This policy should be read alongside the wider suite of Storyy Education policies to ensure a consistent and coordinated approach to safeguarding, digital technology and personal development.

Particular links exist with the:

- Child Protection and Safeguarding Policy
- Positive Behaviour, Relationships and Emotional Regulation Policy
- PSHE and RSHE Policy

- Curriculum Policy
- Attendance Policy
- Mobile Phone and Smart Device Policy
- Equality, Diversity and Inclusion Policy
- Data Protection Policy
- Staff Code of Conduct
- Complaints Policy

Together, these policies provide the framework through which Storyy Education promotes safe, responsible and effective use of digital technology whilst safeguarding children and young people and preparing them for successful participation in modern society.

15. Filtering, Monitoring and Cyber Security

Storyy Education recognises that effective filtering, monitoring and cyber security arrangements form an important part of the organisation's wider safeguarding responsibilities. Whilst technology plays a vital role in reducing exposure to harmful content and identifying potential risks, it does not replace professional curiosity, effective supervision or high-quality online safety education. Filtering and monitoring are therefore implemented alongside the wider safeguarding culture, curriculum and staff vigilance.

Appropriate filtering systems are used to reduce the likelihood of students accessing illegal, inappropriate or harmful online material whilst enabling access to legitimate educational resources. Monitoring arrangements support the identification of safeguarding concerns, inappropriate use of technology, cyber security risks and potential breaches of organisational policies. Any concerns identified through filtering or monitoring will be reviewed promptly and managed proportionately in accordance with the Storyy Education Child Protection and Safeguarding Policy.

Storyy Education is committed to maintaining secure digital systems that protect students, staff and organisational information from unauthorised access, cyber threats and accidental data loss. Staff are expected to maintain secure passwords, use multi-factor authentication where available, protect organisational devices, report suspicious emails or cyber security concerns immediately and ensure that software, operating systems and security updates are maintained appropriately.

Only authorised users may access Storyy Education's digital systems and information. Access permissions are allocated according to individual roles and responsibilities, with confidential information restricted to those who require it to carry out their professional duties. Personal information is managed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the organisation's Data Protection Policy.

The effectiveness of filtering, monitoring and cyber security arrangements is reviewed regularly by senior leaders to ensure that systems remain appropriate, proportionate and responsive to emerging technologies, safeguarding risks and changes in statutory guidance. Lessons learned from incidents, safeguarding reviews, cyber security alerts and technological developments inform continuous improvement across the organisation.

Appendix A – Digital Safety Curriculum Framework

APPENDIX A – DIGITAL SAFETY CURRICULUM FRAMEWORK

This framework outlines the key themes, learning intentions and progression within Storyy Education's online safety curriculum. It is delivered through the RESET and BRIGHT programmes using a stage-not-age approach. Teaching is practical, discussion-based and connected to real-life experiences to build knowledge, skills, resilience and confidence.



CURRICULUM AIMS

To equip learners with the knowledge, understanding and skills to:

- Stay safe, happy and healthy online
- Make informed and responsible digital choices
- Build respectful relationships online and offline
- Think critically about digital content and information
- Protect their identity, privacy and personal information
- Use technology to support learning and future success

CURRICULUM STRAND	KEY LEARNING INTENTIONS	EXAMPLES OF CONTENT	TEACHING APPROACHES	PROGRESSION FOCUS
 1. HEALTHY DIGITAL RELATIONSHIPS	• Understand what respectful online relationships look like • Recognise boundaries and consent • Understand cyberbullying and how to respond	Online communication, friendships, consent, peer pressure, cyberbullying, reporting, blocking and seeking help.	Discussions, scenarios, role play, circle time, mentoring, real-life examples, restorative conversations.	Builds from understanding self and others, to managing peer pressure, to challenging harmful behaviour and supporting others.
 2. KEEPING SAFE ONLINE	• Recognise online risks and hazards • Protect personal information and privacy • Know how to seek help	Privacy settings, passwords, scams, grooming, exploitation, stranger danger, location sharing, inappropriate content, reporting routes.	Interactive activities, quizzes, case studies, trusted adult discussions, problem-solving tasks.	Builds from recognising common risks, to applying safe behaviours, to supporting others and accessing help independently.
 3. DIGITAL CITIZENSHIP	• Understand positive online behaviour • Consider digital footprint and online reputation • Respect copyright and intellectual property	Digital footprint, online reputation, sharing content, online etiquette, copyright, plagiarism, freedom of expression vs. harm.	Group work, debates, reflection tasks, digital citizenship projects, mentoring conversations.	Builds from understanding impact on self, to impact on others, to contributing positively to online communities.
 4. CRITICAL THINKING & ARTIFICIAL INTELLIGENCE	• Evaluate online information and sources • Recognise misinformation and bias • Use AI responsibly and ethically	Misinformation, fake news, influencers, algorithms, deepfakes, AI tools, accuracy, bias, responsible use of AI.	Fact-checking activities, source evaluation, project-based learning, AI exploration with guided reflection.	Builds from recognising unreliable content, to analysing bias and intent, to using AI tools critically and responsibly.
 5. DIGITAL HEALTH AND WELLBEING	• Understand the impact of technology on wellbeing • Develop healthy habits and routines • Recognise when support is needed	Screen time, social media and self-esteem, gaming, online behaviour and emotions, sleep, balance, help-seeking.	Wellbeing activities, self-reflection, goal setting, mentoring, mindfulness exercises, PSHE links.	Builds from awareness of balance, to managing habits, to supporting others and seeking help proactively.
 6. PREPARING FOR ADULT DIGITAL LIFE	• Develop digital skills for education and employment • Understand online economy and security • Build confidence for independent adulthood	Professional communication, online banking awareness, financial scams, cyber security, digital CVs, online job applications, workplace technology.	Project work, real-life tasks, employer inputs, careers education, functional skills integration.	Builds from basic digital participation, to independent use in study and work, to safe and responsible adulthood.

CROSS-CURRICULAR LINKS



PSHE & RSHE
Relationships, wellbeing and personal development



English
Critical reading, communication, online literacy



Maths
Online shopping, budgets, financial understanding



Computing
Digital skills, coding, responsible use of technology



Employability & Careers
Digital skills for study, work and independence

CURRICULUM DELIVERY PRINCIPLES

- ✓ Stage-not-age approach
- ✓ Inclusive and accessible
- ✓ Trauma-informed and relationship-based
- ✓ Practical, discussion-based and contextual
- ✓ Responsive to individual need, risk and lived experience

Note: Content is delivered flexibly and adapted to meet the needs, developmental stage, interests and safeguarding requirements of each learner. Curriculum coverage will be reviewed regularly in response to emerging risks, technology and learner voice.

'We're creating a world where every young person has a brighter future'

Appendix B – Online Risks Progression

APPENDIX B – ONLINE RISKS PROGRESSION

This progression outlines key online risks and the expected understanding, behaviours and support needs at each developmental stage. Teaching is delivered using a stage-not-age approach within the RESET and BRIGHT programmes. Learners may have gaps in previous learning or different life experiences.

ONLINE RISK	EARLY PRIMARY Stage 1 – 2	UPPER PRIMARY Stage 3 – 4	LOWER SECONDARY Stage 5 – 6	UPPER SECONDARY Stage 7 – 8	SUPPORT & INTERVENTION
 CONTACT WITH STRANGERS / ONLINE GROOMING	- Understand that not everyone online is who they say they are. - Know to tell a trusted adult if someone they don't know speaks to them. - Use 'no', 'block' and 'tell' strategies.	- Recognise that some people may try to be friendly for the wrong reasons. - Understand personal boundaries and not sharing private information. - Know how to report and seek help.	- Understand grooming behaviours and manipulation tactics. - Know risks of sharing personal information or images. - Confidently report and support others who may be targeted.	- Understand complex grooming, coercion and exploitation. - Recognise risks across multiple platforms and contexts. - Understand how to support peers and seek professional help.	1:1 mentoring and role play - Safety plans - Multi-agency involvement where required - Targeted education and restorative conversations
 CYBERBULLYING AND ONLINE HARASSMENT	- Understand that unkind words online can hurt. - Know to tell a trusted adult. - Understand how to be kind online.	- Recognise different forms of cyberbullying. - Know how to save evidence and report. - Understand the impact of hurtful messages.	- Understand the emotional impact of cyberbullying. - Know rights, reporting pathways and blocking tools. - Challenge harmful behaviour.	- Understand online harassment, group chats and exclusion. - Know legal implications. - Support others and promote a positive online culture.	- Restorative practice - Behaviour support plans - Pastoral support - Escalation procedures where needed
 SHARING OF PERSONAL INFORMATION	- Understand not to share name, address, school or photos. - Know personal information is private.	- Understand risks of oversharing. - Know what information should remain private. - Understand location sharing risks.	- Evaluate who to share information with and why. - Understand privacy settings and digital footprint. - Know risks of sharing images.	- Confidently manage privacy settings. - Understand long-term impact of sharing information. - Understand risks linked to identity theft and scams.	- Digital literacy sessions 1:1 support - Privacy and boundary coaching
 INAPPROPRIATE CONTENT AND EXPOSURE	- Understand some things online are not for them. - Know to tell a trusted adult.	- Recognise age-inappropriate content. - Understand filters and safe searching. - Know how to report.	- Understand the impact of harmful content. - Use safe search tools. - Know reporting mechanisms.	- Critically evaluate content. - Understand risks of violent, hateful or extremist material. - Challenge harmful content.	- De-escalation support 1:1 mentoring - External agency support if required
 ONLINE SCAMS, FRAUD AND FINANCIAL RISKS	- Understand that not everything online is real. - Know to ask before buying.	- Recognise scams and fake offers. - Understand safe online shopping. - Know not to share payment details.	- Understand phishing, scams and fake links. - Know how to protect accounts and money. - Understand risks in gaming.	- Understand financial fraud, investment scams and subscription traps. - Protect personal and financial data. - Report scams.	- Financial awareness sessions - Digital safety workshops
 ONLINE SEXUAL RISKS (SEXTING, EXTORTION, SHARING IMAGES)	- Understand bodies are private. - Know not to share images. - Tell a trusted adult.	- Understand risks of sharing images. - Know consequences of image sharing. - Understand pressure and coercion.	- Understand sexting, extortion and grooming risks. - Know laws and consequences. - Confidently seek help.	- Understand coercion, extortion and blackmail. - Know legal rights and support services. - Support peers responsibly.	- Specialist safeguarding support - Multi-agency referral - Safety planning
 RADICALISATION, EXTREMISM AND HATE CONTENT	- Understand that some ideas can be unkind or unfair. - Respect differences.	- Recognise unfair stereotypes. - Understand that not everything online is true. - Tell a trusted adult.	- Understand influence and manipulation online. - Recognise extremist content. - Challenge hate and prejudice.	- Understand radicalisation pathways and online propaganda. - Know reporting routes. - Promote tolerance and inclusion.	- PSHE and citizenship lessons - Targeted interventions - Multi-agency support
 EXCESSIVE SCREEN TIME, GAMING AND ADDICTIVE BEHAVIOURS	- Understand balance between screen time and other activities. - Take breaks.	- Understand healthy screen time habits. - Know impact on sleep and wellbeing. - Manage time online.	- Understand impact on mental and physical health. - Set personal limits. - Seek support.	- Understand addiction risks and dopamine cycles. - Use strategies to maintain balance. - Support peers.	- Wellbeing plans - Mentoring and coaching - Referral to wellbeing services

TEACHING AND SUPPORT PRINCIPLES

 TRAUMA-INFORMED Teaching is delivered through trusted relationships, safety, predictability and emotional support.	 STAGE-NOT-AGE Learning is based on developmental stage, understanding and individual needs.	 PRACTICAL AND RELEVANT Real-life scenarios, role play and current technology are used.	 REPETITION AND REINFORCEMENT Key messages are revisited and built on over time.	 EMPOWERMENT Learners are supported to make informed choices and seek help confidently.
--	---	--	---	--

RISK LEVEL KEY

 **LOWER RISK**
Typically manageable through curriculum teaching, universal strategies and positive routines.

 **MODERATE RISK**
Requires additional teaching, monitoring and targeted support for some learners.

 **HIGHER RISK**
Requires targeted intervention, safeguarding oversight and possible multi-agency support.

Note: Content is delivered flexibly and adapted to meet the needs, developmental stage, interests and safeguarding requirements of each learner. Curriculum coverage will be reviewed regularly in response to emerging risks, technology and learner voice.

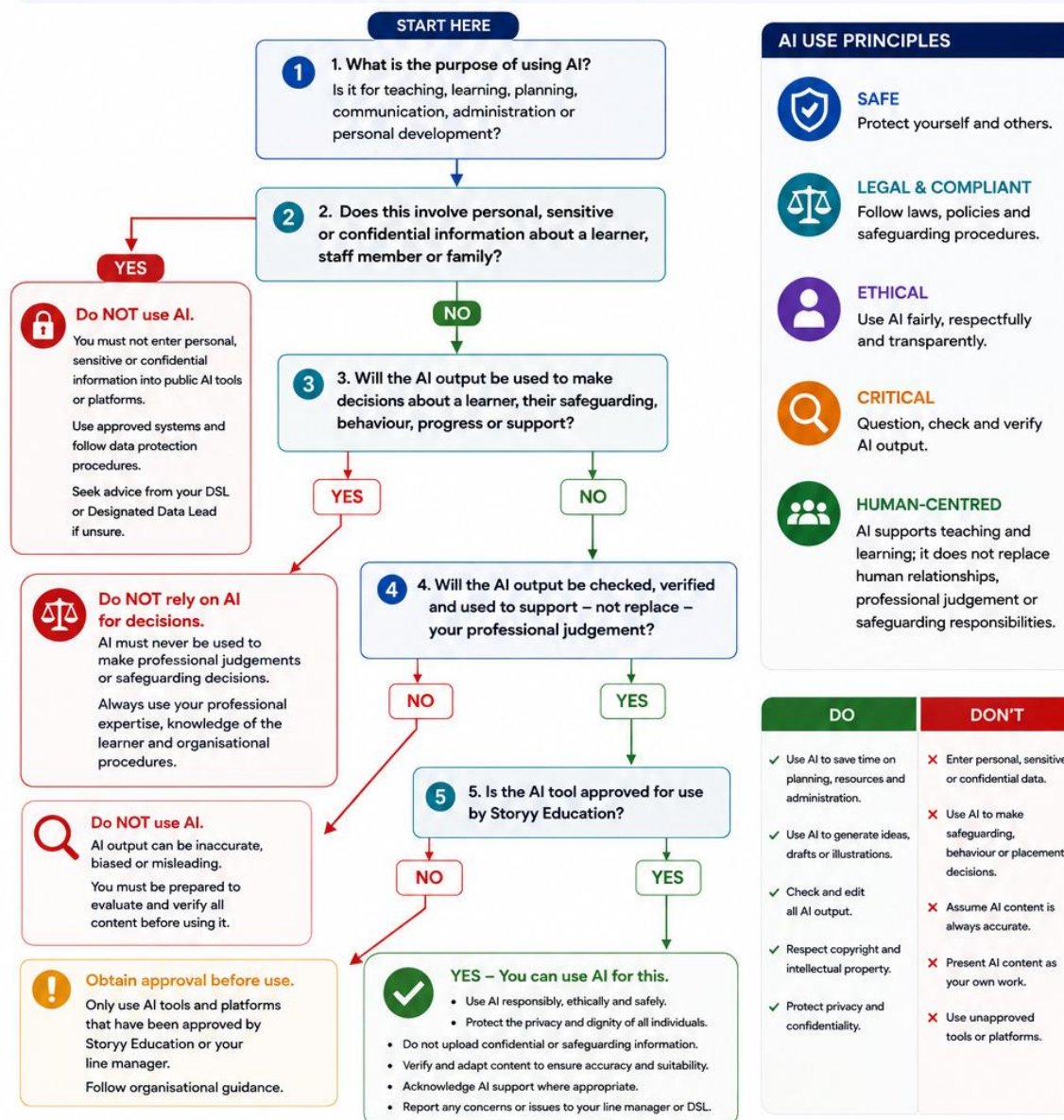
'We're creating a world where every young person has a brighter future'

Appendix C – AI Decision Tree ("Can I use AI for this?")

APPENDIX C – AI DECISION TREE "CAN I USE AI FOR THIS?"



This decision tree supports staff and learners to use Artificial Intelligence (AI) safely, responsibly and appropriately in line with organisational policies, safeguarding responsibilities and data protection legislation.



KEY REMINDERS		EXAMPLES – HOW AI CAN BE USED RESPONSIBLY			
	Never enter confidential or safeguarding information into public AI tools.		TEACHING & LEARNING		ADMINISTRATION
	You are responsible for the content you produce with AI.		- Generate lesson ideas - Create quizzes or activities - Explain concepts in different ways		- Draft emails or letters - Summarise documents - Create checklists or timelines
	Report concerns or inappropriate use. We are all responsible.		RESOURCES & CONTENT		- Create images or diagrams - Adapt text for different learners - Develop presentations
			PERSONAL DEVELOPMENT		- Explore ideas - Brainstorm solutions - Reflect and plan - Build digital skills



If you are unsure at any point, stop and ask.

Contact your Provision Manager, DSL or Designated Data Lead for guidance.

'We're creating a world where every young person has a brighter future'

Appendix D – Online Safety Incident Flowchart

APPENDIX D – ONLINE SAFETY INCIDENT FLOWCHART



Simple, clear steps for responding to online safety concerns.

The safety and wellbeing of children and young people is our priority.



1. CONCERN IDENTIFIED

A concern or disclosure is received from a learner, staff member, parent/carer or through monitoring.



2. CHECK & RESPOND

- Listen, stay calm and take the concern seriously.
- Reassure the individual.
- Do not investigate or ask leading questions.
- Ensure immediate safety if there is a risk.



3. RECORD

Record the concern as soon as possible and certainly within 24 hours on CPOMS. Include factual notes only.



4. REPORT

Inform the Designated Safeguarding Lead (DSL) or Deputy DSL immediately.



5. DSL ASSESSMENT

Does the concern indicate a safeguarding risk?

YES



Safeguarding Risk

- Follow the Child Protection and Safeguarding Policy.
- Consider immediate protective actions.
- Refer to external agencies if required (e.g. Police, MASH, CEOP, LA).
- Inform parents/carers where appropriate and safe to do so.

NO



Not a Safeguarding Risk

- Manage through education, restorative practice and behaviour procedures.
- Support the learner and review any relevant plans or strategies.
- Record actions and follow up as appropriate.



6. FOLLOW UP & REVIEW

- Ensure the learner is supported.
- Review and monitor as appropriate.
- Capture learning and improve practice.
- Record outcomes on CPOMS.



If you are unsure at any point, always report to the DSL immediately.
When in doubt – report it, share it, record it.

KEY PRINCIPLES



SAFETY FIRST

The safety and wellbeing of learners is the priority at all times.



PROPORTIONAL

Respond appropriately to the level of risk and need.



CONFIDENTIAL

Share information only on a need-to-know basis.



COLLABORATIVE

Work with parents/carers, schools and external agencies as required.



LEARNING FOCUSED

Use learning from incidents to improve systems, education and practice.

EXAMPLES OF CONCERNS

- Upsetting or worrying online content
- Cyberbullying or online harassment
- Contact from strangers
- Sharing of images or videos
- Online grooming or manipulation
- Threats or harmful behaviour online
- Inappropriate use of technology
- Sexting or sexual harassment
- Radicalisation or extremist content

WHO IS INVOLVED?



Staff Member

Reports or is notified of the concern.



DSL / Deputy DSL

Reviews, assesses and decides next steps.



External Agencies

Engaged where safeguarding, criminal or welfare risks are identified.

- ✓ Act quickly
- ✓ Keep factual records
- ✓ Follow safeguarding procedures
- ✓ Seek support when needed

'We're creating a world where every young person has a brighter future'

Appendix E – Filtering & Monitoring Escalation Process

