The Lowry Academy
The best in everyone™
Part of United Learning

E-Safety Policy

2026

Aspiration | Resilience | Respect | Confidence | Creativity

E-Safety Policy			
Approved / Accepted by	Adopted template from United Learning by The Lowry Academy (UL Academy School) The Local Governing Board		
Author	Revised by Daniel Hargreaves – AP		
Policy Originator	Rosie Aylward- VP		
Originated/ Adopted	**Accepted by**	**Review Period**	
13.12.2022	Governors	1 Year	
Date to LGB	**Reason**	**Outcome**	**Next review date**
26.03.2024	Annual Review	Ratified & accepted	March 2025
31.03.2025	Annual Review	Ratified & accepted	March 2026
01.04.26	Annual Review	Ratified & accepted	April 2027

1.	**Creating an Online Safety Ethos**
1.1	**Aims and Policy Scope**
	The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provide the platform that facilitates harm. An effective approach to online safety empowers the Academy to protect and educate the whole academy or community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate. a. **content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views; b. **contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and c. **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying. ➢ The Lowry Academy believes that online safety (e-safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. ➢ The Lowry Academy identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. ➢ The Lowry Academy has a duty to provide the academy community with quality internet access to raise education standards, promote student achievement, support professional work of staff and enhance the academy's management functions. TLA also identifies that with this there is a clear duty to ensure that children are protected from potential harm online. ➢ The purpose of The Lowry Academy's online safety policy is to: o Clearly identify the key principles expected of all members of the community with regard to the safe and responsible use of technology to ensure that TLA is a safe and secure environment. o Safeguard and protect all members of TLA Community online. o Raise awareness with all members of the TLA community regarding the potential risks as well as benefits of technology. o To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology. o Identify clear procedures to use when responding to online safety concerns that are known by all members of the community. ➢ This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the academy (collectively referred to as 'staff' in this policy) as well as children and parents/carers. ➢ This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals who have

	been provided with academy issued devices for use off-site, such as a work laptop/ tablet or mobile phones. ➢ This policy must be read in conjunction with other relevant academy policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE)
1.2	**Writing and Reviewing the Online Safety Policy**
	➢ The Lowry Academy's online safety policy has been written by the academy, involving staff, students and parents/carers, building on the United Learning online safety policy template. ➢ The policy has been approved and agreed by the Leadership Team and governing body. ➢ The academy's Online Safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.
1.3	**Key Responsibilities of the Community**
1.3.1	**Key Responsibilities of the Leadership Team** ➢ Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the academy community. ➢ Auditing and evaluating current online safety practice to identify strengths and areas for improvement. ➢ Ensuring there are appropriate and up-to-date policies and procedures regarding online safety. ➢ To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the academy community and ensuring that the filtering and academy network system is actively monitored. ➢ "In accordance with KCSIE, the DSL has **lead responsibility** for understanding how the academy's filtering and monitoring systems operate and for ensuring they are effective." ➢ Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications. ➢ Ensuring that online safety is embedded within a progressive whole academy curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours. ➢ Making appropriate resources available to support the development of an online safety culture. ➢ Taking responsibility for online safety incidents and liaising with external agencies as appropriate. ➢ Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice. ➢ Ensuring there are robust reporting channels for the academy/setting community to access regarding online safety concerns, including internal, local and national support. ➢ Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices. ➢ To work with and support technical staff in monitoring the safety and security of academy systems and networks. ➢ "Filtering, monitoring, and online safety education are adapted to meet the specific needs of vulnerable learners, including SEND and EAL students."

1.3.2	**Key Responsibilities of the Online Safety/Designated Safeguarding Lead (DSL)** ➢ Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate. ➢ Keeping up-to-date with current research, legislation and trends. ➢ Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day. ➢ Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches. ➢ Working with the academy/setting lead for data protection and data security to ensure that practice is in line with legislation. ➢ Through CPOMS, maintaining an online safety incident/action log to record incidents and actions taken as part of the academy's safeguarding recording structures and mechanisms. ➢ Monitoring internet filtering reports to identify behaviour which might indicate safeguarding issues or inappropriate behaviours. Update CPOMS as necessary. ➢ Working with the central IT team to monitor the academy/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the academy leadership team, Governing Body/School Improvement Board and other agencies as appropriate. ➢ Liaising with the local authority and other local and national bodies as appropriate. ➢ Reviewing and updating online safety policies, acceptable use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input. ➢ Ensuring that online safety is integrated with other appropriate academy policies and procedures.
1.3.3	**Key Responsibilities of Staff** ➢ Contributing to the development of online safety policies. ➢ Reading and signing the academy acceptable use Policies (AUPs) and adhering to them. ➢ Taking responsibility for the security of academy/setting systems and data. ➢ Having an awareness of online safety issues, and how they relate to the children in their care. ➢ Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives. ➢ Embedding online safety education in curriculum delivery wherever possible. ➢ Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead. ➢ Knowing when and how to escalate online safety issues, internally and externally. ➢ Being able to signpost to appropriate support available for online safety issues, internally and externally. ➢ Maintaining a professional level of conduct in their personal use of technology, both on and off site. ➢ Taking personal responsibility for professional development in this area. ➢ Software settings - ensuring staff check the settings for software intended to be used, for example platforms are not set to default and allow uses unfiltered access to inappropriate areas. This also includes the use of free software which can have adverts placed on the interface, these adverts could be inappropriate for students. It is the staff teacher's responsibility to personally check the links. ➢ Communication of the importance of secure passwords. ICT team and middle leaders are able to complete password resets for students. ➢ "Filtering, monitoring, and online safety education are adapted to meet the specific needs of vulnerable learners, including SEND and EAL students."

1.3.4	**Additional Responsibilities of Staff Managing the Technical Environment** ➢ Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised. ➢ Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team. ➢ To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on academy-owned devices. ➢ Ensuring that the academy's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL. ➢ Our filtering and monitoring system is reviewed **annually** in line with DfE Filtering & Monitoring Standards (2024) to ensure it accounts for new risks, including AIgenerated harmful content, VPN/proxy bypass attempts, and realtime detection of illegal material." ➢ Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL through these systems. ➢ "In accordance with KCSIE, the DSL has **lead responsibility** for understanding how the academy's filtering and monitoring systems operate and for ensuring they are effective." ➢ Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure. ➢ Checks on appropriate licences to allow staff and students to access the chosen learning platforms and software. ➢ Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures. ➢ Ensuring that the academy's ICT infrastructure/system is secure and not open to misuse or malicious attack. ➢ Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices. ➢ Ensure that appropriately strong passwords are applied and enforced for all but the youngest users. ➢ "Online safety concerns will be managed in line with the Behaviour Policy and Child Protection Policy to ensure a consistent safeguarding response.
1.3.5	**Key Responsibilities of Children and Young People** ➢ Contributing to the development of online safety policies. ➢ Reading the academy/setting Acceptable Use Policies (AUPs) and adhering to them. ➢ Respecting the feelings and rights of others both on and offline. ➢ Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues. At a level that is appropriate to their individual age, ability and vulnerabilities: ➢ Taking responsibility for keeping themselves and others safe online. ➢ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies. ➢ Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.
1.3.6	**Key Responsibilities of Parents/Carers** ➢ Reading the academy/setting acceptable use policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate. ➢ Discussing online safety issues with their children, supporting the academy in their online safety approaches, and reinforcing appropriate safe online behaviours at home. ➢ Role modelling safe and appropriate uses of new and emerging technology.

	➢ Identifying changes in behaviour that could indicate that their child is at risk of harm online. ➢ Seeking help and support from the academy, or other appropriate agencies, if they or their child encounters online problems or concerns. ➢ Contributing to the development of the academy/setting online safety policies. ➢ Using academy systems, such as learning platforms, and other network resources, safely and appropriately. ➢ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2	**Online Communication and Safer Use of Technology**
2.1	**Managing the Website** ➢ The academy will ensure that information posted on the academy website meets the requirements as identified by the Department for Education. ➢ The contact details on the website will be the academy address, email and telephone number. Staff or students' personal information will not be published. ➢ The Principal will take overall editorial responsibility for online content published by the academy and will ensure that content published is accurate and appropriate. ➢ The academy website will comply with United Learning's and the academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright. ➢ The academy will post information about safeguarding, including online safety on the academy website, or link to the resources hosted by United Learning. ➢ The administrator account for the academy website will be safeguarded with an appropriately strong password. ➢ Students' work will only be published with their permission or that of their parents/carers.
2.2	**Publishing Images Online** ➢ The Lowry Academy will ensure that all images are used in accordance with the academy's Image Use Policy. ➢ In line with the academy's Image Use Policy, written permission from parents or carers will always be obtained before images/videos of students are electronically published. ➢ Any images, videos or music posted online will comply with the intellectual property rights and copyright
2.3	**Managing Email** ➢ Students may only use academy/setting provided email accounts for educational purposes. ➢ All members of staff are provided with a specific academy/setting email address to use for any official communication. ➢ Staff are permitted to contact students via their own academy email account and students' academy email accounts during school hours. ➢ Staff must always demonstrate safe and responsible online behaviour. ➢ If communication by a student is deemed to be personal or inappropriate, staff should not respond, and the line manager or safeguarding team should be alerted immediately ➢ The use of personal email addresses by staff for any official academy/setting business is not permitted. ➢ The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider. ➢ Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods. ➢ Members of the academy community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the academy online safety incident log. ➢ Sensitive or personal information will only be shared via email in accordance with data protection legislation. ➢ Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware. If in doubt advice should be sought before opening the email. ➢ Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper would be. Recipients for all emails, especially those sent externally, should be checked carefully before sending.

	➢ Particular care should be exercised when including additional recipients onto an email chain – check all previous emails to minimise the risk of a data breach. ➢ Academy email addresses and other official contact details will not be used for setting up personal social media accounts.
2.4	**Appropriate Safe Classroom Use of the Internet and Associated Devices** ➢ The academy's internet access will be designed to enhance and extend education. ➢ Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students. ➢ Students will use age and ability appropriate tools to search the Internet for content. ➢ Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole academy curriculum. ➢ The academy will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information. ➢ All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use are essential. ➢ All academy owned devices will be used in accordance with the academy Acceptable Use Policy and with appropriate safety and security measure in place. ➢ Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. ➢ The academy will use age appropriate search tools as decided by the academy following an informed risk assessment to identify which tool best suits the needs of our community. ➢ The academy will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment. ➢ Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. ➢ The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-academy/setting requirement across the curriculum. ➢ Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
2.5	**Management of Academy Learning Platforms (LP)** ➢ SLT and staff will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities. ➢ Students/staff will be advised about acceptable conduct and use when using the LP. ➢ Only members of the current student, parent/carers and staff community will have access to the LP. ➢ All users will be mindful of copyright issues and will only upload appropriate content onto the LP. Please also refer to the point raised regarding licensing and software settings to ensure filtering and monitoring systems are secure. ➢ When staff, students etc. leave the academy their account or rights to specific academy areas will be disabled or transferred to their new establishment. ➢ Any concerns about content on the LP may be recorded and dealt with in the following ways: o The user will be asked to remove any material deemed to be inappropriate or offensive. o The material will be removed by the site administrator if the user does not comply. o Access to the LP for the user may be suspended. o The user will need to discuss the issues with a member of leadership before reinstatement. o A student's parent/carer may be informed.

	➢ Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.
3	**Policy Decisions**
3.1	**Recognising Online Risks** ➢ The Lowry Academy's is aware that the Internet is a constantly changing environment with new applications, tools, devices, sites and material emerging at a rapid pace. ➢ Emerging technologies will be examined for educational benefit and the academy leadership team will ensure that appropriate risk assessments are carried out before use in academy is allowed. ➢ The academy will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content. Academy's should include appropriate details about the systems in place. ➢ The academy will audit technology use to establish if the Online Safety (e–Safety) Policy is adequate and that the implementation of the policy is appropriate. ➢ Methods to identify, assess and minimise online risks will be reviewed regularly by the academy's leadership team. ➢ Filtering decisions, internet access and device use by students and staff will be reviewed regularly by the DSL ➢ "Our filtering and monitoring system is reviewed **annually** in line with DfE Filtering & Monitoring Standards (2024) to ensure it accounts for new risks, including AI-generated harmful content, VPN/proxy bypass attempts, and real-time detection of illegal material." ➢ Online safety concerns will be managed in line with the Behaviour Policy and Child Protection Policy to ensure a consistent safeguarding response.
3.2	**Internet Use Within the Community** ➢ The academy will liaise with United Learning and local feeder academies to establish a common approach to online safety (e–Safety). ➢ The academy will provide an Acceptable Use Policy for any guest/visitor who needs to access the academy computer system or internet on site.
3.3	**Authorising Internet Access** ➢ The academy will maintain a current record of all staff and students who are granted access to the academy's electronic communications. ➢ All staff, students and visitors will read and sign the Academy Acceptable Use Policy before using any academy ICT resources. ➢ Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability. ➢ Parents will be asked to read the Academy Acceptable Use Policy for student access and discuss it with their child, where appropriate. ➢ When considering access for vulnerable members of the academy community (such as with children with special education needs) the academy will make decisions based on the specific needs and understanding of the student(s).
4	**Engagement Approaches**
4.1	**Engagement of Children and Young People** ➢ An online safety (e-Safety) curriculum will be established and embedded throughout the whole academy, to raise awareness regarding the importance of safe and responsible internet use amongst students. ➢ Education about safe and responsible use will precede internet access. ➢ Students input will be sought when writing and developing academy online safety policies and practices. ➢ Students will be supported in reading and understanding the academy Acceptable Use Policy in a way which suits their age and ability.

	➢ All users will be informed that network and Internet use will be monitored. ➢ Student instruction regarding responsible and safe use will precede Internet access. ➢ Online safety (e-Safety) will be included in the PSHE and Computing programmes of study covering safe usage both within the academy and externally. ➢ Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments. ➢ The student acceptable use expectations and Posters will be posted in all rooms with Internet access. ➢ Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas. ➢ External support will be used to complement and support the academy's internal online safety (e-Safety) education approaches. ➢ The academy will reward positive use of technology by students. ➢ The academy will implement peer education to develop online safety as appropriate to the needs of the students.
4.2	**Engagement of Staff** ➢ The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of academy safeguarding practice. ➢ To protect all staff and students, the academy will implement Acceptable Use Policies which highlights appropriate online conduct and communication. ➢ Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential. ➢ Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis. ➢ The academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students. ➢ Training- Staff are provided with training and opportunities to practice using software/systems intended to be implemented during remote learning. Training is ongoing led through the Teaching and Learning team on effective pedagogies they can use in an online environment. ➢ All members of staff will be made aware that their online conduct out of academy could have an impact on their role and reputation within academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
4.3	**Engagement of Parents/Carers** ➢ The Lowry Academy recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology. ➢ Parents' attention will be drawn to the academy's Online Safety (e-Safety) policy and expectations in newsletters, the academy prospectus, social media and on the academy website. ➢ Parents will be requested to read online safety information as part of the Home Academy Agreement. ➢ Parents will be encouraged to read the academy Acceptable Use Policy for students and discuss its implications with their children. ➢ Information and guidance for parents on online safety will be made available to parents in a variety of formats. ➢ Parents will be encouraged to role model positive behaviour for their children online. ➢ Training- Parents/carers will also receive training in school methodology in using Office 365, Teams, Streams etc.

	➢ Parents will be receiving regular communication through various systems, twitter, Facebook group, website, email/letter with regarding Microsoft Office 365 tools and expectations from students.
5.	**Responding to Online Incidents and Concerns**
	➢ All members of the academy/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc). ➢ "Online safety concerns will be managed in line with the Behaviour Policy and Child Protection Policy to ensure a consistent safeguarding response." ➢ The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. ➢ The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to the United Learning Designated Safeguarding Officer and relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures. ➢ Complaints about Internet misuse will be dealt with under the Academy's complaints procedure. ➢ Complaints about online bullying will be dealt with under the Academy's anti-bullying policy and procedure ➢ Any complaint about staff misuse will be referred to the Principal ➢ Any allegations against a member of staff's online conduct will be referred to the Principal. ➢ Students, parents and staff will be informed of the academy's complaints procedure. ➢ Staff will be informed of the complaints and whistleblowing procedure. ➢ All members of the academy community will need to be aware of the importance of confidentiality and the need to follow the official academy procedures for reporting concerns. ➢ All members of the academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the academy community. ➢ The academy will manage online safety (e-Safety) incidents in accordance with the academy discipline/behaviour policy where appropriate. ➢ The academy will inform parents/carers of any incidents of concern as and when required. ➢ After any investigations are completed, the academy will debrief, identify lessons learnt and implement any changes as required. ➢ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the DSL will refer to local safeguarding partners or Local Police via 999 if there is immediate danger or risk of harm. ➢ The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to United Learning Technology Team and Local Police. ➢ If the academy is unsure how to proceed with any incidents of concern, then the incident will be escalated to the United Learning Lead Safeguarding Officer or Local Education Safeguarding Team. ➢ If an incident of concern needs to be passed beyond the academy, then the concern will be escalated to the Local Safeguarding partner and, if relevant, the Trust safeguarding team. ➢ Parents and children will need to work in partnership with the academy to resolve issues. ➢ Concerns related to **online safety or cyberbullying** should be reported through **CPOMS.** ➢ **Anonymous reporting** for students is available through **the school's reporting system.**

	➢ External agencies, such as **Internet Watch Foundation (IWF) and NSPCC**, can be contacted for additional support.
6.	**Filtering and Monitoring**
	➢ The Lowry Academy uses SmoothWall to filter and monitor internet usage. ➢ "The academy implements a proactive monitoring strategy, including automated alerts, staff review processes, and clear protocols for responding to flagged incidents, in line with KCSiE. ➢ Filtering settings are reviewed quarterly by the IT Network Manager, in conjunction with the DSL and Digital Strategy Lead [responsible staff/IT team] to ensure compliance with KCSIE. ➢ "Our filtering and monitoring system is reviewed **annually** in line with DfE Filtering & Monitoring Standards (2024) to ensure it accounts for new risks, including AI generated harmful content, VPN/proxy bypass attempts, and real-time detection of illegal material." ➢ The academy ensures that legitimate educational content is not blocked ("overblocking"). ➢ Breaches of the filtering and monitoring systems flagged by the AI are automatically alerted to the DSL and other members of the safeguarding team for review and action. ➢ Breaches of the filtering and monitoring systems are flagged to the DSL and Headteacher for review and appropriate actions. ➢ Any breaches or filtering **concerns should be reported immediately to [Designated Safeguarding Lead and the IT Department]** ➢ "Filtering, monitoring, and online safety education are adapted to meet the specific needs of vulnerable learners, including SEND and EAL students."
7.	**Remote Learning**
	➢ In the circumstance that learning is conducted remotely, it must: ➢ Be done via the approved platform (Microsoft TEAMS) ➢ Staff should follow camera and recording guidance to maintain privacy and appropriate safeguarding controls. ➢ Parental supervision is recommended where necessary.
8.	**Cybersecurity and Data Protection**
	➢ Staff and students must use strong passwords, and staff should use 2 factor authentication where possible. ➢ Personal data must be encrypted when stored or shared electronically. ➢ The academy complies with the **UK GDPR & Data Protection Act 2018.** ➢ Any data breaches must be reported immediately to the **Data Protection Officer.**
9.	**AI and Emerging Risks**
	➢ AI-generated content (e.g., ChatGPT, should be used **responsibly** and **fact-checked before sharing**. ➢ Students should be educated on the **risks of misinformation** and manipulated media. ➢ The use of AI in the classroom must comply with **academic integrity.** ➢ "The academy recognises the risks of AI generated content, including deepfakes, grooming risks, misinformation and harmful imagery. Staff and students will be trained to recognise AI manipulated content and report concerns.