Ascend Learning Trust

Online Safety Policy

Policy Owner:	Head of IT
Date of issue:	November 2024
Policy Level:	Tier 1
Approved by:	Full Trust Board
Next Review:	November 2027[i]

Contents

Version Control

Version	Details	Author	Date
1.0	Policy formation	Kyle Gaskin	1st September 2024
2.0	Policy Change: Addition of filtering and monitoring section	Jeremy Masson (following DPE feedback)	30th October 2024
3.0	Office Manager details updated	Charlotte Mercer	April 2025
4.0	Updates for AI, Misinformation and Disinformation	Kyle Gaskin	05th February 2026

Related Policies

- Child Protection and Safeguarding Policy (school specific)
- Behaviour Policy (school specific)
- Disciplinary Policy
- Ascend Cyber Security Policy
- Ascend Data Protection Policy
- Ascend ICT & AUP Policy
- Ascend AI Policy
- Privacy Notice for Workforce
- Privacy Notice for Students
- Privacy Notices for General
- Complaints Policy
- Staff Code of Conduct

Introduction

This Ascend Learning Trust Policy applies to Ascend Learning Trust as a whole and to all the schools in the Trust.

It is the responsibility of the Local Governing Body and Headteacher of each school, and the Board of Trustees and CEO for Trust Shared Services, to ensure that everyone adheres to this policy. In implementing the policy and associated procedures the Local Governing Body, Headteacher and Trust staff must take account of any advice given to them by the ALT Trust IT Lead, the ALT CEO and/or Board of Trustees.

This Policy is subject to the Scheme of Delegation approved for Ascend Learning Trust. If there is any ambiguity or conflict then the Scheme of Delegation and any specific Scheme or alteration or restriction to the Scheme approved by the Board of Trustees, takes precedence.

If there is any question or doubt about the interpretation or implementation of this Policy, the ALT Trust IT Lead should be consulted.

Policy Statement

Ascend Learning Trust and its schools understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, can provide pupils with the opportunity for learning through collaboration. Whilst the Trust recognises the

importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.
This policy is to ensure the online safety of all children, staff members, trustees, volunteers, and visitors.

This will be accomplished through:

- Robust processes in place to ensure the online safety of everyone.
- Deliver an effective approach to online safety, cross Trust, which empowers us to protect by establishing clear mechanisms to identify, intervene and record.
- Providing clear boundaries of acceptable online behaviour.
- Appropriate use of Trust resources, both internally and remotely.
- Provide clarity of when schools should intervene with online safety issues. Regular information sharing and sign posting for parent advice.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation, Teaching about relationships, sex and health and Sharing nudes and semi-nudes: advice for education settings working with children and young people.

For additional information and guidance, please refer to the links above.

Roles and Responsibilities

School	Staff member	Role	Contact details
Ascend Learning Trust	K Gaskin	Trust IT Lead	kgaskin@ascendlearningtrust.org.uk
Royal Wootton Bassett School	Zach Ishani	E-Development and Digital Lead	zishani@rwba.ascendlearningtrust.org.uk
Lawn Manor Academy	Marek Koza	Assistant Headteacher	mkoza@kga.ascendlearningtrust.org.uk

Kingsbury Green Academy	Lorna Karby	Office Manager	lkarby@kga.ascendlearningtrust.org.uk
The Wellington Academy	Vicky Fawdry	Data Lead	victoriafawdry@twa.ascendlearningtrust.org.uk
Wellington Eagles Primary	Claire Keilty	Office Manager	clairekielty@wps.ascendlearningtrust.org.uk
Wellington Lions Primary	Denise O'Brien	Office Manager	deniseobrien@wps.ascendlearningtrust.org.uk
Noremarsh Junior School	Karen Beard	Office Manager	kbeard@njs.ascendlearningtrust.org.uk

*Appendix 1 Reporting Concerns Flowchart

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at least annually.

Trust Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding and child protection policy.

Reporting will be overseen by the DSL / DDSL / OSL

The Executive Team/The Trust Board

The Executive Team has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Executive Team will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Trust Board members will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see Ascend ICT & Acceptable Usage Policy).

The Headteacher / Principal

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school, with guidance from the Online Safety Lead.

The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead

Details of the school's DSL, DDSL and OSL are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school through engagement with the Online Safety Lead.
- Working with the headteacher, Trust IT Support and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of online bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Safeguarding recording software entries that are related to Online behaviours or incidents are shared with the Online Safety Lead when/if appropriate.
- Updating and delivering staff training on online safety with support from the Online Safety Lead.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or Trust Board with input from the Online Safety Lead.

This list is not intended to be exhaustive.

The Online Safety Lead

The lead for online safety is responsible for:

- Ensuring effective teaching and learning of online safety.
- Ensuring online safety issues are embedded in all aspects of the school.
- Raising awareness of online safety issues within the school and wider community.

Trust IT Support

The Trust IT Support team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis, blocking access to potentially dangerous sites and where possible preventing the downloading of potentially dangerous files.
- Ensuring that the Trust IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
  Ensuring that any online safety or cyber-bullying incidents are referred to the relevant parties as described in this policy. This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.

- Adhering to this policy consistently alongside the Trust ICT & Acceptable Usage Policy.
- Ensure that any online safety or cyber-bullying incidents are logged.
- Making sure that children are regularly reminded of their responsibilities regarding online safety and behaviour.
- Support pupils to critically evaluate online content and challenge harmful or misleading information where it impacts wellbeing or safeguarding.
- Be alert to emerging online risks, including AI-generated content, misinformation, disinformation and online conspiracy narratives, and respond in line with safeguarding procedures.

This list is not intended to be exhaustive.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the technology in an appropriate way. The Trust will support parents to understand these issues through parents' evenings, newsletters, letters, website, social media, and information about national/local online safety campaigns/literature.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on the Trust ICT & Acceptable Usage policy.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Help & Advice for Parents - Childnet International
- Parent Zone - Parent Zone | At the heart of digital family life

Visitors and members of the community

Visitors and members of the community who use the Trust IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on IT and Acceptable Usage and Mobile Telephones.

All staff should be aware of the content of this policy, and how it applies to themselves, children Parents/Guardians, Visitors, and members of the community.

Educating children about online safety

Children will be taught about online safety and the potential harm, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Children will receive the help and support of the school to recognize and avoid online safety risks and build their resilience.

Children will be taught the breadth of issues categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example, pornography, fake news, AI-generated misinformation, disinformation, conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  Contact: being subjected to harmful online interaction with other users; for example, peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Children will be also taught to recognise and manage risks linked to misinformation, disinformation and AI-generated content, including content designed to mislead, manipulate opinions or present false narratives as fact.

This includes developing skills to:

- Question the reliability and intent of online information
- Understand that AI-generated content may appear realistic but be inaccurate or false
- Recognise conspiracy theories and online narratives that promote fear, mistrust or harm
- Know how and where to report concerning or confusing content

The computing curriculum covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Children should learn what positive, healthy and respectful relationships look like, following a scheme of work. In addition, teachers will also respond to any particular issues and concerns with individuals and classes as and when they arise, referring to the Online Safety Lead when appropriate.

Key online safety messages will also be reinforced across all areas of the curriculum. Children will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information. Children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Schools will use assemblies to raise children's awareness of the dangers that can be encountered online and may also invite speakers to talk to children about this.

The Trust will raise parents' awareness of online safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via online link on Trust website.

Educating parents about online safety

There is information about keeping children safe online (including social media, apps, and gaming) available on the Trust School websites.

Emerging Technologies and Online Influence

The Trust recognises that emerging technologies, including artificial intelligence, present new safeguarding challenges. These may include the creation or spread of misleading, manipulated or false content, online impersonation, and the amplification of harmful narratives or conspiracy theories.

The Trust is committed to:

- Educating pupils and staff about these risks
- Monitoring developments in technology and guidance
- Updating safeguarding responses where online influence may negatively affect pupils' safety, wellbeing or decision-making

Child on Child abuse via digital technologies

All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school and online. All staff should be clear as to the school's policy and procedures about child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Child-on-child abuse via digital technologies is most likely to include, but may not be limited to:

- Bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)

Keeping Children Safe in Education references the following for guidance: https://www.farrer.co.uk/globalassets/clients-and-sectors/safeguarding/addressing-child-onchildabuse.pdf

Digital Communications

The Trust expects that all staff will ONLY communicate with Students and Parents via secure Trust approved systems, that can be monitored.
Where these are outside or pre-existing relationships, please refer to the Staff Code of Conduct Policy.

Acceptable use of the internet in school

Where a child misuses the Trust Technology, we will follow the procedures set out in the ICT Acceptable Usage Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses Trust technology or a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and our allegations management policy. Action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.
All children, parents, staff, volunteers, Members and Trustees are expected to sign the Trust acceptable use policy. Use of Trust technology must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by children, staff, volunteers, LAB members, Trustees and visitors to ensure they comply with the above.

Filtering and Monitoring

As outlined in our Child Protection and Safeguarding Policy, the trust has appropriate filtering and monitoring arrangements in place that meet our statutory obligations outlined in Keeping Children Safe in Education. The trust IT support team is responsible for ensuring that an appropriate system is in place both within the central team and at each school, and ensuring that procedures are updated in accordance with legislative changes or updates to statutory guidance.

Filtering and Monitoring systems utilised by the trust allow for the centralised monitoring of websites visited by all users on trust based devices. As aforementioned, by using trust based IT systems, users both understand and consent that filtering and monitoring systems will be used to safeguard users.

Filtering and Monitoring software will operate at all times and will alert nominated users if a breach is detected. This may be due to an attempt to access a website that has been blocked, or is barred; a trigger word has been detected on an online search or within the content of a website or a trigger word has been detected within written correspondence, such as an e-mail.

The trust IT support team will routinely monitor the filtering and monitoring software and will alert key staff where concerns have arisen. At school level alerts will be sent to the Headteacher and DSLs and within the central team, alerts will be sent to the CEO.

Filtering and monitoring systems should be configured to identify risks associated with AI-generated content, including deepfake imagery, impersonation, manipulated media, and content designed to mislead or influence pupils.

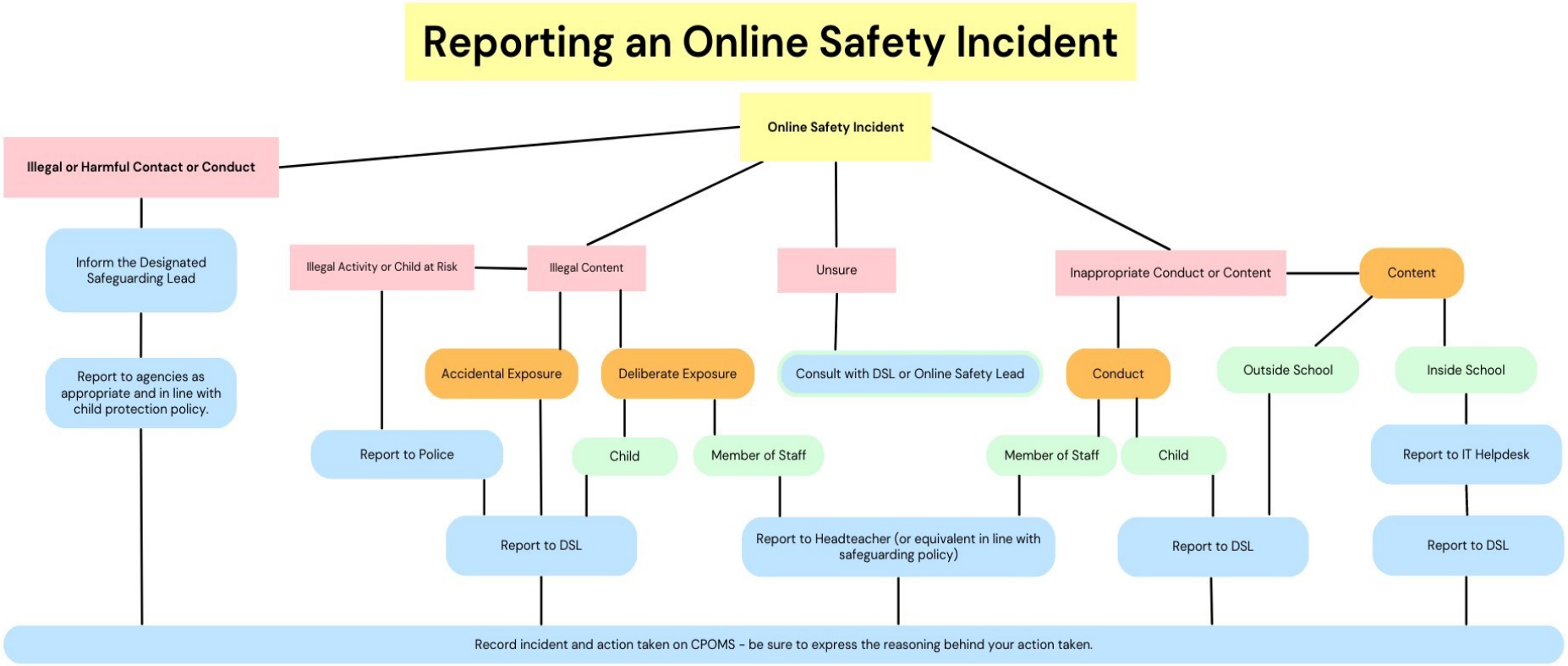
The responsibility to investigate concerns linked to filtering and monitoring will fall to the aforementioned post holders. Where the concern is linked to a student, the safeguarding team will be made aware and may support with discussions at student level. An entry must also be made to CPOMs with the appropriate linked category to ensure that a holistic view around the safeguarding of that child can be gathered.

Where the concern links to a member of staff, the line manager may be asked to discuss the concern. A conversation can normally determine the reason for the trigger; where the concern gives rise to a more substantial concern around the conduct of a member of staff and may indicate a breach of policy, advice should be sought from HR and action will be taken as appropriate in line with the acceptable use policy and code of conduct.

From time to time, teachers may observe or discover that students have been able to access a website that would be deemed inappropriate. Where the filtering and monitoring system has not blocked this website, the staff member is responsible for notifying the central IT support team so that the website can be added to the appropriate block list.

Filtering and Monitoring systems are regularly ‘stress tested’ by the safeguarding team within each school (at least each half term) working in partnership with the IT support team. As part of the safeguarding monitoring by local governing bodies, an annual check of filtering and monitoring will take place. Both LGB and school based monitoring should ensure that filtering and monitoring tests are conducted using a range of devices (laptops, ipads, desktop pcs, etc) and in a range of scenarios (such as wireless connectivity from different parts of the school site).

Appendix 1 – Reporting Concerns Flow chart



[i] *The responsible officer must keep the policy or procedure current between formal reviews. Minor or technical changes to a policy or procedure that do not affect its substance may be made by the responsible officer without requiring approval from the approving body. Examples include updating staff names, contact details, or making technical adjustments required by legislation or guidance that do not alter how the policy or procedure works. If a proposed change is substantial and does not qualify as a minor or technical drafting amendment, the revised policy or procedure must be submitted to the next available meeting of the approving body for consideration and approval.*