Ascend Learning Trust

Online Safety Policy 2023-24

This policy applies to all students, staff and visitors.

Written by: A collaboration of members from the Safeguarding Leads, IT Leads, the Executive Team and the DPO

Date Ratified by ALT:		10th May 2023
Version Number:		1
Committee Reviewed:		ALT Trustees
Policy Type:		Tier 2 Template
Date ratified by LGB	:	24th January 2024
Adopted by:		Kingsbury Green Academy
Review Date:		Annually

Contents

Quick Reference Contacts Guide

	Name	Contact Details
Designated Safeguarding Lead (DSL)	Elvy Johnson	ejohnson@kga.ascendlearningtrust.org.uk
Head teacher / Principal	Jason Tudor	Principal@kga.ascendlearning trust.org.uk
Deputy Designated Safeguarding Lead (DDSL)	Adrian Roberts	aroberts@kga.ascendlearningtrust.org.uk
Designated Information Technology Lead (DITL)	Vicki Scott	vscott@kga.ascendlearningtrust.org.uk
Data Protection Officer (DPO)	Mark Harrison	dpo@ascendlearningtrust.org.uk

Aims

Our school aims to:
Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'). Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as 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, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nude and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation & 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 DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there

is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

This policy MUST be read in conjunction with the :

- Acceptable Use Agreement KS3-KS5 April 2023
- Acceptable Use Agreement Staff, Visitors, Contractors April 2023

Roles & Responsibilities

The Trust & Governing Board

The Trust board is responsible for making sure there is a policy in place and the local governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board 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) and the designated information technology lead (DITL). The governor who oversees online safety is the Governor responsible for Safeguarding. All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's IT (Information Technology) systems and the internet. (see separate acceptable use agreements).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND (Special Educational Needs & Disabilities) because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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
- Working with the headteacher, designated information technology lead, IT lead, data protection officer and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school child protection policy and data protection policy
- Ensuring that any online safety incidents are logged on CPOMS (secure platform containing all safeguarding or child protection concerns) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)
- The annual Certificate for Online Safety is provided by The National College for all staff.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the headteacher and/or LGB

This list is not intended to be exhaustive.

The IT network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, including filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Applying forced password changes for all users regularly, as a minimum every 6 months for staff and a minimum of 12 months for secondary students. Primary students do not require password changes. Note that schools who have implemented Multi Factor Authentication (MFA) are not required to apply forced password changes.
- Applying a minimum password security strength of at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) using Microsoft guidance with complexity requirements turned on.
- Applying forced screen lock to all school devices (i.e. desktops, laptops) after more than five minutes of inactivity.
- Ensuring that all school fixed and portable devices (i.e. desktops, laptops) have been encrypted.
- Ensuring that all school devices have the latest anti-virus and spyware software installed.
- Ensuring that all school devices have the latest operating system updates installed.
- Ensuring that the school's IT systems are secure, up to date and protected against viruses, malware and spyware and that such safety mechanisms are reviewed and updated regularly.
- Conducting a full security check and monitoring the school's IT systems on a regular basis.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy – all Entries are logged on CPOMS.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Ensuring that any personal data breaches are reported to the data protection officer and dealt with appropriately in line with the data breach procedure.

This list is not intended to be exhaustive.

All staff and volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Ensuring that any personal data breaches are reported to the data protection officer and dealt with appropriately in line with the data breach procedure.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Ensure that they and their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet. (see separate acceptable use agreements) Notify a member of staff or the headteacher of any incidents or concerns they have regarding their child's use of the internet including social media.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy, which can be requested from the school as noted in the acceptable use agreement.

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

- What are the issues? – UK Safer Internet Centre (UKSIC)
- Hot topics – Childnet International
- Keeping Children Safe Online – NSPCC

Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use agreement (see separate acceptable use agreements).

Educating Pupils about Online Safety

Pupils will be taught about online safety through:

- KS3 (Key Stage 3) IT Lessons
- KS4 (Key Stage 4) lessons for CS and IT
- KS5 (Key Stage 5) lessons for CS and IT
- PSHE Days

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact, and conduct, and know how to report concerns
- How to install antivirus and malware packages
- How to understand the difference between fake and real news
- Understand the dangers of online gaming, gambling and live streaming
- How to use social media currently and for its intended purpose
- Recognise the laws behind using technology and how to conform to these

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- How to be able to install software to protect their devices
- The ethical and legal responsibilities of using online technologies
- Online consent and legal age requirements
- The dangers of excessive use of online technologies, such as online gaming and the effect it could have on student's health.

Pupils in Key Stage 5 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

- How to be able to install software to protect their devices
- The ethical and legal responsibilities of using online technologies
- Online consent and legal age requirements
- The dangers of excessive use of online technologies, such as online gaming and the effect it could have on student's health.
- Appropriateness of sharing photos online and the recent changes in the law.

By the end of secondary school, pupils will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn. (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant including PSHE days.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will:

- Raise parents' awareness of internet safety in letters, communications home, and in information via our website.

- Share suitable materials with parents when there has been an issue with a student or group of students.
- Make this policy available to parents on request.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Child on Child Abuse

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors, Pupil Managers or Head of Year will discuss cyber-bullying with pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also shares information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so. When necessary, the incident will be reported to the relevant social media platform to be taken down.

Examining electronic devices

Senior staff in schools have the specific power under the Education and Inspections Act 2006 and the Education Act 2011 to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or report it to the police
- Inform parents/carers

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation.
- UKCIS (UK Council for Internet Safety) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure. https://kingsburygreenacademy.com/wp-content/uploads/2023/10/KGA-Complaints-Policy-Sept-2023.pdf

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers, contractors and governors are expected to sign an acceptable use agreement (either electronically or in paper format) regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet 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 pupils, staff, volunteers, governors, contractors and visitors (where relevant) to ensure they comply with the above.

Staff and students must agree and sign to the acceptable use agreement

Pupils Using Mobile Devices in School

Students are not allowed to use their mobile phones during the school day. If a phone is seen, used or heard during the school day by a member of staff, then it will be confiscated until the end of the school day when students can collect it from the Student Hub. If the offence is repeated, parents/carers will be asked to come in and collect it. In some lessons, a teacher may feel that the mobile phone can support the learning of the classroom. If this takes place the teacher will clearly state that mobile phones can be used for the task of the learning.

Staff Using Work Devices Outside of School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Not installing any software without the explicit written agreement of the school's IT team.
- Not leaving the device unattended, for example in a remote office or car.
- Not sharing the device with anyone else.
- Reporting any alerts relating to malware or a virus to the school's IT team as soon as possible.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in their acceptable use agreement.
Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must seek advice from the Network Manager

HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use. Any incident that is deemed a safeguarding concern will also be recorded on CPOMS. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The Subject Leader for IT and Computing will be notified of the issue

- A decision will be made for the consequence
- All blocked internet will be recorded on Arbor/SIMS with the Time frame
- The Class Teacher, Head of Year or Subject Leader for IT and Computing will contact home.

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Ascend Learning Trust's Code of Conduct. The 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.

TRAINING

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, e-bulletins, and staff meetings).

By way of this training, all staff will be made aware that:
Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages.
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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 regular intervals, and at least annually. The Subject Leader IT and Computing will advise the DSL in this area and will continue to update their CEOP training.

Governors 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 child protection and safeguarding policy.

MONITORING ARRANGEMENTS

The Trust will ensure annual audits are carried out to ensure this policy is being followed by schools. Audits will be carried out by the DPO and by IT contractors as instructed by the CFO.

The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed every year by the DSL and link Governor for Safeguarding.

At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

Appendix 1 Online Safety Training Needs - Self Audit for Staff

Name of staff member/volunteer:	Date:
Question	Yes / No (please also add any comments here)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware that your IT department is responsible for protecting the school network with appropriate content filtering and firewalls against cyber-attack? A cyber-attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or device with the intent to cause intentional damage.	
Do you know the name of the person or department you must report a phishing email or cyber-attack to? Do you also know the out of hours emergency contact details to report an attack or a concern?	
Are you aware that if your email or Microsoft 365 account (i.e. Outlook, SharePoint) has been compromised (accessed) by a third party via any form of cyber-attack that you must report this immediately to your IT support department, your line manager and your DPO?	

Are you aware of the ways pupils can abuse their peers online? Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you aware that you can report inappropriate student or staff access to the internet sites to your IT support department who are responsible for filtering and monitoring school access to external sites and blocking them if necessary?	
Are you aware that you must not download any external applications to your school device without the explicit written approval of your IT support department?	
Are you familiar, and have you signed the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you aware that Multi Factor Authentication (MFA) to access certain platforms within the school and Trust, will become an accepted and mandated process?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Are you aware of how to report a personal data breach and to who?	

Please return to your Office Manager in your first month of employment or before.

Guide to abbreviations:

- ALT – Ascend Learning Trust
- DITL – Designated Information Technology Lead
- SEND – Special Educational Needs & Disabilities
- CPOMS – Secure platform for recording and monitoring safeguarding and child protection concerns
- IT – Information Technology
- LGB – Local Governing Body
- UKCIS – UK Council for Internet Safety
- DfE – Department for Education
- KS3 – Key Stage 3 (age 11 to 14)
- KS4 (Key Stage 4 (age 14 to 16)
- DSL – Designated Safeguarding Lead
- PSHE – Personal Social Health and Economic