Online Safety Policy

Anderida Learning Centre

Approved by:	Mathew Thompson	**Date:** 4th November 2024
Last reviewed on:	04/09/2026	
Next review due by:	03/09/2027	

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 5
5. Educating parents about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 8
9. Staff using work devices outside school 8
10. How the school will respond to issues of misuse 9
11. Training 10
12. Monitoring arrangements 11
13. Links with other policies 12
14. Key Contacts 14

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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, conspiracy theories, misinformation, disinformation, 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-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. 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 Head of Centres 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head of Centre to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

Ensure 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 (appendix 3)

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

3.2 The Head of Centre

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

3.3 The Designated Safeguarding Lead

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 Head of Centre in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of Centre and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Head of Centre 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of Centre and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT contact

The ICT contact is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files through the filtering system
- Ensuring that any online safety incidents are logged (see appendix 5) 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes by reporting to the DSL.
- Informing the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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
- 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.

3.6 Parents

Parents/carers are expected to:

- Notify a member of staff or the Head of Centre of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

Upon admission, a letter, information leaflet, and factsheet will be sent home to parents/carers. Knowledge of online safety will be reviewed regularly and latest information will be sent out with long term progress reports. This includes any new apps or developments in applications that affect online safety for pupils and parents.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach Relationships and sex education and health education in secondary schools

In **KS3**, 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

Pupils in **KS4** 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

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
- About the online risks relating to disinformation, misinformation, and conspiracy theories
- Not to provide material to others that they would not want shared further and not to share personal material that 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 that 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.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher (Billy Mc Inally), the DSL (Jaz Profit), or the school's Online Safety Officer (Vinny Miles).

The school's Online Safety Officer Vinny Miles will keep parents/carers informed of updates, as well as supporting any concerns regarding online safety. Information and support will be shared via email and post with resources such as posters, leaflets, and information notices.

Concerns or queries about this policy can be raised with any member of staff or the Head of Centre.

6. Cyber-bullying

6.1 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.)

6.2 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Head of Centre, and any member of staff authorised to do so by the Head of Centre can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Head of Centre

Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

Seek the pupil's co-operation and also the parents/carer's approval - it will always be the preference that Parents/Carers conduct any searches.

Authorised staff members may examine an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Head of Centre / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching students will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

ALC recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

ALC will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the School.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors have access and will be guided on the Online Safety Policy. 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 and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

The school recognises that mobile phones are an important part of young people's everyday lives and can support communication, independence and emotional security. However, inappropriate use can negatively affect learning, behaviour and safeguarding.

While we recognise the statutory guidance within Keeping Children Safe in Education (KCSIE) regarding restrictions on the use of mobile phones in schools, we have adopted a proportionate and needs-led approach that reflects the specific characteristics of our SEMH provision.

We work under the premise that, for some of our pupils with social, emotional and mental health needs, removing access to mobile devices may create a barrier to attendance and engagement. Decisions regarding pupil access to mobile phones will therefore be informed by safeguarding considerations, individual needs, and professional judgement, with the best interests of the child remaining paramount at all times.

Young people at ALC are not provided with internet access through school devices or the school network and are therefore not permitted to connect personal mobile phones to the school's Wi-Fi.

Young people are encouraged to put their mobile phones away during lessons to support engagement with learning. Outside of lessons, they are permitted to use their phones appropriately during the school day, provided this does not disrupt learning, compromise safeguarding, or negatively affect others.

Any use of mobile devices in school by pupils must align with the behaviour policy.

Specialist SEN and alternative provision approach

ALC operates within a specialist SEN and alternative provision context, where a significant priority is to enable young people to attend school and engage with education. For some young people, particularly those who have experienced significant barriers to education, a completely mobile-phone-free environment could create an additional boundary and potentially become a barrier to attendance and engagement.

Our approach therefore seeks to balance safeguarding and educational responsibilities with the individual needs of the young person and the primary purpose of our provision. We do not currently operate a completely mobile-phone-free environment. Instead, we encourage young people to develop appropriate boundaries around their phone use, particularly during lessons, while allowing reasonable access at other appropriate times.

This does not mean that inappropriate or unsafe use is accepted. Where phone use disrupts learning, involves inappropriate content, creates a safeguarding concern or breaches school expectations, staff will respond appropriately and proportionately.

Any safeguarding concerns arising from mobile phone use, including cyberbullying, online harassment, exploitation, coercion or the sharing of nude or semi-nude images, will be managed in accordance with this policy.

The school will keep its mobile phone arrangements under review in line with current Government guidance and legislation.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

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 Head of Centre or DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour policy and ICT 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 the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff 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.

11. 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- 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

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.

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 and when applicable.

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

12. Filtering and Monitoring arrangements

Filtering and monitoring systems are used to keep pupils safe when using your school's IT system. Filtering systems block access to harmful sites and content. Monitoring systems are used to identify when a user accesses or searches for certain types of harmful content on school devices.

The school uses Securly to ensure that students are protected from harmful and inappropriate online content wherever they are learning. For more information, please refer to their website. The school's Online Safety Officer Vinny Miles has access to the platform, and reviews and monitors arrangements as necessary and in line with statutory requirements.

Whenever pupils are using a school device, they will be physically monitored at all times as the school works on a 1:1 basis.

A member of the SLT and a governor will be responsible for making sure the standards are met and kept. Jaz Profit is the allocated person for ALC.

Incidents of misuse on school laptops will be written up on an online safety incident log (see appendix 4) which is available in the safeguarding folder on the school system. Incidents will also be logged under "incidents" in the school's daily logs and interventions will be taken accordingly based on individual needs and support. A copy of reports will be stored securely in the pupil's safeguarding files.

This policy will be reviewed every year by the DSL. 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.

We audit our systems annually to ensure the fully comply with current Government guidance

13. Links with other policies, legislation, guidance and documents

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints policy
- ICT and internet acceptable use policy
- Anti-bullying policy

Other Information and documentation

- Online Safety Act
- Government guidance filtering and monitoring

- Internal Annual Filtering and Monitoring review

14. Key Contacts

Role	Name	Contact details
Online safety officer	Vinny Miles	vinny.miles@anderidalearningcentre.co.uk
Designated Safeguarding Lead	Jaz Profit	07713 695 284 jaz.profit@anderidalearningcentre.co.uk
Deputy Designated Safeguarding Lead	Toby Patton	Toby.patton@anderidalearningcentre.co.uk
Deputy Designated Safeguarding Lead	Rebecca Corradetti	Rebecca.Corradetti@anderidalearningcentre.co.uk
Headteacher	Billy Mc Inally	Billy.mcinally@anderidalearningcentre.co.uk
Nominated governor safeguarding & child protection	Micheal Mc Glynn	Mcgkynnigan@hotmail.co.uk
Chair of governors	Annabel Lilley	Lilleymeister@hotmail.co.uk
Local Authority Designated Officer (LADO)	Donna Davis	lado@eastsussex.gov.uk
Safeguarding Officer and Assistant LADO	Susan Giles	07543 237465
Adult LADO	Kellie Clarke	01323 747310
Referrals into Early Help and Social Care	Single Point of Advice (SPoA)	01323 464222 0-19.SPoA@eastsussex.gov.uk Out of hours: 01273 335906/01273 335905 Adult services: 01323 636399
Multi Agency Safeguarding Hub (MASH)		01273 290400
Other		Designated Doctor Safeguarding Children: 01424 758012 Designated Nurse Safeguarding Children: 01424 735664 Designated Nurse LAC: 01323 446999