Online Safety Policy

Atypical Education

Approved by:	Emma Oxnam	**Date:** 1st September 2022
Last reviewed on:	4th September 2023	
Next review due by:	4th September 2024	

Contents

1. Aims

Atypical Education aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- Deliver a practical approach to online safety, which empowers us to protect and educate the whole community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones)
- Establish precise mechanisms to identify, intervene and escalate an incident where appropriate

The four 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, antisemitism, 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 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 pornography), sharing other graphic images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 cyberbullying 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 Owner

The owner monitors this policy and holds the staff accountable for its implementation.

All staff will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the ICT systems and the internet (Appendix 3)

- Ensure that online safety is a running and interrelated theme while devising and implementing their approach to safeguarding and related policies and procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Designated Safeguarding Lead

Details of the designated safeguarding lead (DSL) are in our child protection and safeguarding policy.

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

- Supporting and ensuring that staff understand this policy and that it is being implemented consistently
- Working with the staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the child protection policy
- Ensuring that any online safety incidents are logged 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 behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and external services if necessary

3.3 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated regularly
- Ensuring that the ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially hazardous files
- Ensuring 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 behaviour policy

3.4 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of ICT
- 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 behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and harassment, both online and offline and maintaining an attitude of ‘it could happen here.’

3.5 Parents

Parents are expected to:

- Notify a member of staff of any concerns or queries regarding this policy
- Ensure their child understands and agrees to the terms of acceptable use of the internet

Parents 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 International
- Parent resource sheet – Childnet International

3.6 Visitors and members of the community

Visitors and community members who use the ICT systems or the internet will be made aware of this policy when relevant and expected to read and follow it. They will be expected to agree to acceptable use terms if appropriate.

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Other relevant subjects will also cover the safe use of social media and the internet.

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 about online safety

Atypical Education will let parents know:

- What their children are being asked to do online
- What sites they will be asked to access
- Who their child will be interacting with online

If parents have any queries or concerns concerning online safety, these should be raised in the first instance with the DSL.

Concerns or queries about this policy can be raised with any staff member.

6. Cyber-bullying

Cyberbullying occurs online through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyberbullying, 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 to report incidents and are encouraged to do so, including where they are a witness rather than the victim.

Atypical Education will actively discuss cyberbullying with pupils, explaining why it occurs, the forms it may take, and the consequences. 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 and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils as part of safeguarding training.

Atypical Education will follow the processes set out in the behaviour policy about a specific incident of cyber-bullying; where illegal, inappropriate or harmful material has been spread among pupils, we 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.

6.1 Examining Electronic Devices

Staff have the specific power under the Education and Inspections Act 2006 (which has been increased by 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
- Disrupt teaching, and

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 the material, or
- Retain it as evidence (of a possible criminal offence*) and
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that is a criminal offence to possess, they will not view the image but will report this to the DSL immediately, who will decide what to do next. The DSL will align 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.

** Staff will also confiscate the device to give to the police if they have reasonable grounds to suspect that it contains evidence about an offence.

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

- 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

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be handled through the complaints procedure.

7. Acceptable use of the internet

All pupils, parents, staff and volunteers are expected to agree on the acceptable use of ICT systems and the internet.

Internet use must be for educational purposes only or to fulfil 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.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices

Pupils may bring and may use mobile devices for educational purposes but are not permitted to use them during the following:

- Lessons

Any use of mobile devices by pupils must align with acceptable usage.

9. Staff using work devices

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 eight 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 permanently installing the latest updates

10. Responses to issues of misuse of ICT

When a pupil misuses the ICT systems or the Internet, we follow our ICT and Internet acceptable use policy procedures. The action will depend on the specific incident's circumstances, nature and seriousness and will be proportionate.

Where a staff member misuses the ICT systems, the internet, or a personal device where the action constitutes misconduct, the staff code of conduct will deal with the matter. The action taken will depend on the specific incident's circumstances, nature and seriousness.

Consider whether incidents involving illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

As part of their induction, all staff members will receive training on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training and 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 well-being issues, and 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 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 up the risks
- 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 will undertake child protection and safeguarding training every two years, including online safety. They will also update their knowledge and skills on online safety regularly and at least annually. Volunteers will receive appropriate training and updates, if applicable.

Our child protection and safeguarding policy sets out more information about safeguarding training.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by Emma Oxnam.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the ICT systems (like computers) and get onto the internet, I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use computers for schoolwork only
• Be kind to others and not upset or be rude to them
• Look after the ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that Atypical Education will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the ICT systems and internet when appropriately supervised by a staff member. I agree to the conditions set out above for pupils using the ICT systems and the internet, and I will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the ICT systems (like computers or phones) and get onto the internet, I will:** • Always use the ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present or with a teacher's permission • Keep my usernames and passwords safe, and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites, including social networking sites, chat rooms and gaming sites, unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails or follow any links in emails without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer or without adult supervision **If I bring a personal mobile phone or other personal electronic device:** • I will not use it during lessons, tutor group time, clubs or other activities without a teacher's permission • I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that Atypical Education will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the ICT systems and internet when appropriately supervised by a staff member. I agree to the conditions set out above for pupils using the ICT systems and internet and for using personal electronic devices, and I will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, VOLUNTEERS AND VISITORS	
Name of staff member/volunteer/visitor:	
When using the ICT systems and accessing the internet on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Share my password with others or log in using someone else's details • Take photographs of pupils without checking with teachers first • share confidential information with its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share	
I will only use the ICT systems and access the internet on a work device for educational purposes or to fulfil my role's duties. I agree that Atypical Education will monitor the websites I visit and use the ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school hours and keep all data securely stored by this policy and the data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others. I will also do so if I encounter any such material. I will always use the ICT systems and internet responsibly and ensure that pupils in my care do so.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**