Online Safety Policy

LEARNING

Approved by:	Active Learning	Active Learning
Last reviewed on:	01/09/2023	01/09/2023
Next review due by:	01/09/2024	01/09/2024

Contents

1. Aims

Our organisation's aims are to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole organisation 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, 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 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 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 organisations on:

- Teaching online safety in organisations
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and organisation 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 students’ electronic devices where they believe there is a ‘good reason’ to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The directors and trustees

The directors and trustees have overall responsibility for monitoring this policy and are accountable for its implementation.

The directors/trustees will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

Head of IT Administration & Online Safeguarding oversees all digital online safety (Richard Clark).

The DSL has overall responsibility for implementing all safeguarding procedures.

All directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the organisation’s ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing the organisation’s approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children/young people, victims of abuse and students with SEND because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children/young people in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The director(s)

The directors are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation.

3.3 The designated safeguarding lead

Details of the organisation’s designated safeguarding lead (DSL) 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 the organisation, in particular:

- Supporting the directors in ensuring that staff understand this policy and that it is being implemented consistently throughout the organisation

- Working with the directors, IT Administration and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the organisation 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 cyberbullying are logged and dealt with appropriately in line with the organisation 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 organisation to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Head of IT Administration

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 on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while using the organisation's resources, including terrorist and extremist material
- Ensuring that the organisation'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 organisation's ICT systems on a [weekly] 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 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 organisation 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
- Agreeing and adhering to the terms on acceptable use of the organisation's ICT systems and the internet (appendix 3), and ensuring that students follow the organisation's terms on acceptable use (appendices 1 and 2)
- 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 organisation 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/Guardians

Parents/Guardians are expected to:

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

Parents/Guardians 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

3.7 Visitors and members of the community

Visitors and members of the community who use the organisation's ICT 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 acceptable use (appendix 3).

4. Educating students about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All organisations have to teach:

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

Primary organisations:

students in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary education**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary organisations:

In **Key Stage 3**, students 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

students 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

By the **end of secondary education**, students 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.

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

5. Educating parents/guardians about online safety

The organisation will raise parents'/guardians' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE) [Google Classroom/zoom/Teams]. This policy will also be shared with parents.

Online safety will also be covered during parents' meetings.

The organisation will let parents know:

- What systems the organisation 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 organisation (if anyone) their child will be interacting with online

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

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

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the organisation behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The organisation will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/tutors will discuss cyber-bullying with their tutor groups.

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, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The organisation also sends information/leaflets 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 organisation will follow the processes set out in the organisation behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the organisation 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 organisation has 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 students' 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 organisation 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 leadership team to decide whether they should:

- Delete the material, or

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

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this 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.

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

Any searching of students 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

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the organisation complaints procedure.

7. Acceptable use of the internet in organisation

All students, parents, staff, volunteers and Directors are expected to sign an agreement regarding the acceptable use of the organisation's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the organisation's terms on acceptable use if relevant.

Use of the organisation'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 students, staff, volunteers, trustees 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. Students using mobile devices in organisation

Students may not use personal mobile devices when working with the organisation, the organisation provides tracked and monitored devices for all students.

Any use of mobile devices when working with the organisation by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the organisation behaviour policy, which may result in discontinuation of services.

9. Staff using work devices outside organisation

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 install the latest updates

Staff members must not use the device in any way which would violate the organisation'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 IT Administration (itsupport@metronomeeducation.org)

10. How the organisation will respond to issues of misuse

Where a student misuses the organisation's ICT systems or internet, we will follow the procedures set out in our student and parent agreements. 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 organisation'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 disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The organisation 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
- 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 students can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy 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.

Directors 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the directors At every review, the policy will be shared with the trustees. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour agreement
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Student and parent user agreement

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (students and parents/carers)

UNDER DEVELOPMENT

Appendix 2: acceptable use agreement (staff, Directors, volunteers and visitors)

UNDER DEVELOPMENT

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in your organisation?	
Are you aware of the ways students can abuse their peers online?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the organisation’s acceptable use agreement for staff, volunteers, Directors and visitors?	
Are you familiar with the organisation’s acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the organisation’s ICT systems?	
Are you familiar with the organisation’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

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**