Online Safety Policy

Written by	**DPO – Neil Packard**
Approved by	**Board of Directors (Original Summer 2018, updates Autumn 2020)**
Review - Annually	**Autumn 2022**
Next Review	**Autumn 2023**

Contents

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of students, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

The policy also takes into account the National Curriculum computing programmes of study.

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

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Principal 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 sage guarding governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2)

3.2 The Principal

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

3.3 The Designated Safeguarding Lead

Details of the Academy's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged in the bully incident log and dealt with appropriately in line with the Academy PD (behaviour) policy

- Updating and delivering staff training on online safety (appendix 3 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 the Academy to the Principal and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting full security checks and monitoring the Academy's ICT systems on continual 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 in the bullying incident log and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy PD (behaviour) policy and passed to the Personal Development team

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 Academy's ICT systems and the internet (appendix 2), and ensuring that students follow the Academy's terms on acceptable use (appendix 1)
- 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

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the Academy 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 2).

4. Educating students about online safety

Students will be taught about online safety as part of the computing curriculum, and through the online safety yearly plan.

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
- 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

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

The Academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

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

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

Concerns or queries about this policy can be raised with the Principal/DSL.

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 Academy's PD (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 Academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health, citizenship and economic (PSHCE) education (covered within Citizenship lessons), and other subjects where appropriate.

All staff and governors receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The Academy also sends information physically and electronically 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. A monthly online safety newsletter is sent out as well an annual Digital Parenting magazine (Parent Zone).

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy PD (behaviour) policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavours to ensure the incident is contained and dealt with.

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.

6.3 Examining electronic devices

Academy 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 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 school rules

If inappropriate material is found on the device, it is up to 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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in the Academy

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the Academy 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, 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 and 2.

8. Students using mobile devices in the Academy

Student mobile phones, electronic devices and accessories e.g. earphones and smart watches, should be out of sight and switched off while in the School. On arrival, children put their phone in the class box which is then transported to reception for safe keeping.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB devices must not be used to store or move school data. USB devices are banned in school and must not be connected to school computers.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. How the Academy will respond to issues of misuse

Where a student misuses the Academy ICT systems or internet, we will follow the procedures set out in the behaviour 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 Academy 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Academy 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. See appendix 1 for Prevent information.

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).

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 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.

This policy will be reviewed every two years by the Vice Principal (Curriculum). At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding (child protection) policy

- PD (behaviour) policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: PREVENT (Online radicalisation)

What is the PREVENT strategy?

PREVENT is a government strategy designed to stop people becoming terrorists or supporting terrorist or extreme causes. The PREVENT strategy covers all types of terrorism and extremism, including the extreme right wing, violent groups and other causes.

How does the PREVENT strategy apply to schools?

From July 2015, all schools have a duty to keep children safe from radicalisation and extremism. This means we have a duty to protect them from extreme and violent views in the same way that we protect them from drugs or gang violence. In school, we can provide a safe place for children to discuss these issues so they have a better understanding about how to protect themselves.

What does this mean at Marsden Junior School?

Many of the things we already do in school to help our children become positive, happy members of society also contribute to the PREVENT strategy, these include:

- The encouragement of open discussion throughout the school, particularly in our PSHE lessons.
- Challenging prejudices and racist comments.
- Developing critical thinking skills and a strong, positive self-identity.
- Children are taught to listen to others with tolerance whilst discussing their own opinions. They are taught to respect the views of others and other ways of life.
- Exploring other cultures and religions and promoting diversity.
- In computing lessons, children are taught to question what they read on the internet.
- Children are encouraged to talk to an adult about things that worry or confuse them.
- Promoting the spiritual, moral, social and cultural development of ALL pupils, as well as British Values such as democracy.
- We will also protect children from the risk of radicalisation, for example by using filters on the internet to make sure they cannot access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.

How does PREVENT relate to British values?

Schools have been actively promoting British Values since 2014. British values include: democracy, the rule of law, individual liberty and mutual respect, and tolerance (acceptance) of different faiths and beliefs.

The PREVENT strategy is not just about discussing extremism itself, which may not be suitable or appropriate for younger children. It is also about teaching fundamental British Values such as tolerance, respect, democracy and the rule of law. School staff ensure that all discussions are appropriate for the age and maturity of the children involved.

Is extremism really a risk in our area?

Extremism can take many forms. It can be linked to politics, religion, colour of skin or nationality. Therefore, we will try to give our children the skills to protect them from any extremist views they may encounter, now or later in their lives.

Key Terms

Extremism – vocal or active opposition to fundamental British values such as democracy, the rule of law and tolerance of different faiths and beliefs.

Ideology – a set of beliefs.

Terrorism – a violent action against people or property, designed to create fear and advance a political, religious or ideological cause.

Radicalisation – the process by which a person comes to support extremism and terrorism.

Useful resources:

PREVENT duty guidance www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Frequently asked questions, Prevent For Schools www.preventforschools.org

What is Prevent? Let’s Talk About It http://www.ltai.info/what-is-prevent/

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the Academy ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the Academy ICT systems and accessing the internet in the Academy, or outside the Academy on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the Academy's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the Academy network using someone else's details

I will only use the Academy's ICT systems and access the internet in the Academy, or outside the Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the Academy will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Academy, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Academy's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

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

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are you aware of PREVENT? Briefly explain	
Are there any areas of online safety in which you would like training/further training? Please record them here.	