Online Safety Policy 2021

The Moorlands Primary Federation

TMPF
THE MOORLANDS
PRIMARY FEDERATION

Reviewed:	Oct. 2021	**Date:**	
Approved:	Dec.2021		
Next review due by:	Oct. 2022		

Contents

....

1. Aims

Our Trust aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Trustees;

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

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

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

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the Trust Leadership Team to account for its implementation.

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the school's Designated Safeguarding Lead (DSL).

The Trustee who oversees online safety is: Benjamin Fabi

All Trustees will:

Ensure that they have read and understand this policy;

Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 2);

3.2 The School Leaders

The School Leaders are 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 Designated Safeguarding Lead (DSL) [and deputy/deputies] are set out in our TMPF Safeguarding Policy 2021.

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

Supporting the School Leader/Principal/Executive Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;

Working with leaders, Computing Co-ordinators, Systems Technician and other staff, as necessary, to address any online safety issues or incidents;

Ensuring that any online safety incidents are logged (see appendix 4) 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 Trust's 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 school to the Executive Principal and/or Trust Board.

This list is not intended to be exhaustive.

3.4 The Systems Technician

The Systems Technician is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including radicalisation material;

Ensuring that the school's IT 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 IT systems on a monthly 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 4) and dealt with appropriately in line with this policy;

Report any incidents of cyber-bullying to School Leaders.

This list is not intended to be exhaustive.

3.5 All staff (including supply teachers, Associate Teachers) 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 school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1);

Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

Notify a member of staff or the School Leader 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 IT 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

Information also exists on the school website.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:
Use technology safely and respectfully, keeping personal information private;
Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils 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.

The safe use of social media and the internet will also be covered in other subjects where relevant. Each school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications and via our website, letters, emails, leaflets or parental workshops. This policy will also be available to parents and carers via our website.

When necessary, online safety will also be covered during parents' evenings or workshops.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher then School Leader or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the School Leader/Principal/Executive Principal.

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 TMPF 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 aim to educate children so that they know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Each 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. Staff will discuss cyber-bullying with their children, 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 may include personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, members of the Trust Board 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).

Each school also sends information/leaflets on cyber-bullying and e-safety to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected. Schools will also offer parent workshops when and where appropriate.

Information about online safety can be found on TMPF's website.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Trust's 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 managed appropriately.

The School Leader or DSL/DDSL will report incidents 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

School 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/or
Disrupt teaching; and/or
Break any of the school rules/ work against the school culture and ethos.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
Delete that material or
Retain it as evidence (of a criminal offence or a breach of school discipline); and/or
Report it to the police.

Any searching of pupils 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 pupils' electronic devices will be dealt with through TMPF Complaints Policy.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Trust Board Members are expected to sign an agreement regarding the acceptable use of the school's IT 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 school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We monitor the websites visited by pupils, staff, volunteers, Trust Board Members 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. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

Lessons;
Clubs before or after school, or any other activities organised by the school;
For security reasons, all devices must be handed into the school office.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with TMPF Behaviour Policy, which may result in the confiscation of their device.

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, or breach TMPF Code of Conduct.

Staff must ensure that their work device is secure and password/code 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. Any USB devices containing data relating to the school must be encrypted or not used.

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the TMPF 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 school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/TMPF 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 – Prevent.

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 deputy/deputies] will undertake child protection and safeguarding training, which ought to 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, ideally at least annually.

Trust Board Members 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 TMPF 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 4.

This policy will be reviewed termly by the Trust Leadership Team. At every review, the policy will be shared with the Trust Board.

13. Links with other policies

This online safety policy is linked to:

TMPF Safeguarding Policy

TMPF Behaviour Policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

TMPF Code of Conduct

Removal of Equipment from Premises Agreement

TMPF Confidentiality Policy

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

Pupil's IT Acceptable User Policy

The school has computers and other devices that enable internet access and facilitate our learning.

These rules will keep everyone safe and help us to be fair to others.

- I will only login as myself.
- I will only open and view my files, or files I have permission to use.
- I will not copy other people's work or anything that is protected by copyright.
- I will use the school IT equipment for school work and homework only.
- I will not download from an external storage device, such as memory stick/drive, or the internet without permission.
- I will ask permission before I use the internet.
- When using school IT equipment, I will only communicate with people whom a member of staff has approved.
- The 'communication' I send will be polite, responsible, kind and appropriate.
- I will not give anyone my address, phone number or any other personal information.
- I will report any unpleasant materials or communication sent to me. I know that my report would be to help protect myself and other pupils.
- I understand my school 'online activity' is being monitored.

Child's name: ....

I understand and agree to these rules.

Signed ....(child)   Date............................

I understand why the school has these rules, have discussed them with my child and agree to them.

Signed ....(parent) Date ....

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

Acceptable use of the school's IT systems and the internet: agreement for staff, Trustees, volunteers and visitors

Name of staff member/ Trust Board Members /volunteer/visitor:

When using the school's IT systems and accessing the internet in school, or outside school 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 school's or Trust's reputation;

Use any improper language when communicating with external organisations online, including in emails or other messaging services;

Install any unauthorised software;

Share my password with others or log in to the school's network using someone else's details (unless granted by work colleagues;

Allow non-staff members to use school or Trust resources.

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, 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 IT manager know if a pupil 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 intend to use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/ Trust Board Members /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 pupil 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 pupils and parents?	
Do you regularly change your password for accessing the school's IT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident