MILTON MOUNT SCHOOL

GREENSAND MULTI ACADEMY TRUST

Online Safety and Acceptable Use of Technology Policy

Approved by:	Local School Committee	Date: 1st July 2025
Last reviewed on:	27th June 2025	
Next review due by:	June 2026	

Contents

Rationale

At Milton Mount Primary School, we ensure the safety and wellbeing of children and staff is paramount when they are using the internet, social media or mobile devices/smart technology. We will support and encourage children to use the internet, social media and mobiles in ways that they can enjoy, keeps them safe and shows respect for others. Children, parents and staff will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. We will support and encourage parents and carers to do what they can to keep their children safe online. We provide information on the school website which signposts parents to organisations which offer guidance and advice about online safety. Online Safety training is scheduled in staff meetings throughout the year, so teachers have the confidence and resources they need to deliver internet safety education and to effectively safeguard students. Parents are also kept up to date with online safety advice and guidance.

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, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:
Key Stage 1 and Key Stage 2 will have 5 online safety sessions a half term that cover the areas highlighted by the Education for a Connected World document.

The online safety curriculum is split into 8 different categories:

- Self-image and identity
- Online relationships
- Online Reputation

- Online Bullying
- Managing Online Information
- Health, well-being and lifestyle
- Privacy and Security
- Copyright and ownership

In addition to these areas -

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

By the end of primary school, pupils 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

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters in communications home. 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 head teacher and/or the DSL.

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
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.

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

Roles and Responsibilities

The Headteacher

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

Online Safety Team

Milton Mount has an Online Safety Team responsible for the implementation of this policy. Members include the DSL; PSHE Leader and Computing Leader

The Team meets half termly and works cohesively to implement online safety practise across the school and report regularly to the online-safety Governor.

Working as part of the online safety team, the Computing lead is responsible for:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the local school committee to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead with the DSL on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the Computing leader and school technical support to make sure the appropriate systems and processes are in place
- Working with the DSL 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 headteacher and/or local school committee
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

The Designated Safeguarding Team

Details of the school's designated safeguarding team are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The Local School Committee

The local school committee has responsibility for monitoring the content and implementation of this policy and holding the headteacher to account. The responsibility for co-ordinating this will be held by the nominated safeguarding governor.

The local school committee will also monitor with school leaders whether staff have received 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 local school committee 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 local school committee 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 local school committee should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The local school committee must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness, including:

- 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 School's Acceptable Use Policy
- 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

All Staff and Volunteers

All 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 ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
  - Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
  - 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 failing.
- Following the correct procedures by contacting the Computing lead 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 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’

Parents/carers

Parents and carers are responsible for ensuring that their children are accessing safe and age-appropriate content at home, monitoring children’s social media use and raising concerns with the school where they arise.

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
- Internet Matters

Acceptable use of technology in school

All pupils, parents and staff are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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.

Children in the school have a year group log in to access the school network, which in turn provides filtered access to the internet. Year 5 and 6 children have their own log in and password to access the school network. The children have their own password to access Purple Mash (our computing software) and they are taught to keep passwords private and to understand that sharing a password can result in someone using their access inappropriately.

Children and parents are encouraged to use the educational links on the school website.

Nobody is permitted to access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; lifestyle websites e.g. that promote anorexia or self-harm; any other information which may be illegal or offensive to colleagues. This is reviewed by JSPC regularly.

It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should a pupil access any of these sites unintentionally children should report the matter to a member of staff so that it can be logged on the JSPC helpdesk and CPOMs. We also encourage the children to turn the screen off if they see anything that they don't think is appropriate so that the teacher can log the website on the JSPC log for it to be blocked. If a member of staff inadvertently accesses a site, they must log it on the JSPC helpdesk.

Access to any of the following should be reported to West Sussex Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.
Staff are aware that internet use and emails may be subject to monitoring.

Any suspected virus outbreaks should be reported to the Senior Leadership Team, who will ensure that JSPC (the school network manager) is informed as soon as possible.

Use of smart devices in school

Year 6 and Year 5 pupils may bring smart devices, such as mobile phones to school. These must be given to their class teacher for the duration of the school day.

Reporting Concerns and responding to misuse

Staff are aware of how to report safeguarding concerns via CPOMs in relation to any online issues.

Where a pupil misuses the school ICT systems or internet, we will follow the procedures set out in our behaviour policy according to the details, nature and seriousness of the incident.

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 Standards of Conduct policy. 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.

Throughout the year staff receive safeguarding training on online bullying, abuse, radicalisation and extremism and know how it can be reported.

At the beginning of each academic year the computing curriculum starts with a unit based on online safety and all children are reminded about the user agreement which encourages children to report concerns.

Children are taught to turn the screen off immediately if they inadvertently come across inappropriate content or a contacted inappropriately. They should then report the incident immediately to a member of staff who will inform a member of the Leadership team. The Leadership team will contact JSPC to block the website or will report the incident to the police if deemed serious enough.

We participate in Anti-bullying Week and Safer Internet Day which focuses on how to support children online.

Our school website signposts parents to sites where they can find additional information or report concerns e.g. The Safer Internet Centre, Parent Zone, CEOP and Internet Matters.

The school is committed to acting upon any online safety incidents outside the school that affect the well-being of our pupils or staff members.

Cyber- bullying

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.

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.
All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

We are committed to acting on online safety and online bullying incidents that occur both in and out of school and will take appropriate actions.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

The process is:

- The teacher and parents will be informed
- The incident will be logged on CPOMS
- Parents will be called in for a meeting if the Leadership team think it is necessary or if an incident happens more than once

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 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.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device, under the conditions set out within our Behaviour Policy.

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.
Milton Mount 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.
Milton Mount will treat any use of AI to bully pupils in line with our 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.

Social media

The school may use social media platforms to share children's achievements and other items of educational value.
Children's photographs will only be included in posts if parents have signed permission forms for the images to be used on the internet.

School will remove a photograph of a child as soon as possible if their parents request this.

We acknowledge that staff might use social networking sites for personal use out of school. We advise that they bear in mind security of personal details, rather than relying on the default settings. Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that personal profiles are not publicly available. They should not post about school in any negative way or in any way that would bring the school into disrepute.

Using personal accounts, members of staff, student teachers, work experience students and volunteer helpers should never knowingly become "friends" with pupils on any social networking site or engage with pupils on internet chat.

Staff are advised to decline friend requests from parents.

Children are taught that there are minimum age limits to sign up for social networking accounts and that this is for their safety.

Use of Email

All members of staff should use their professional email address for conducting school business with outside agencies.

Parents use classteacher@miltonmount.co.uk to email teachers. These emails are checked before being passed onto staff.

Staff using work devices outside of 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
  Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.
If staff have any concerns over the security of their device, they must seek advice from JSPC.

Where a member of staff must take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. Staff should log in to the secure remote access to the school network from home, rather than carry unencrypted personal data.

All personal data will be handled according to the Data Protection Act 2018

Staff are permitted to use school ICT equipment for personal use if the use complies with all other points of this policy.

Passwords

Staff should keep school passwords private. Passwords are confidential and individualised to each person.

On no account should a member of staff allow a pupil to use a staff login.

We recognise that at times people without logins will need them. New staff awaiting a login should use one of the supply teacher logins.

Images and Videos

Staff and pupils should not upload onto any internet site (including social media sites) images or videos of themselves or other staff or pupils without consent, including photos of staff which may cause embarrassment or bring the school into disrepute.

Any images or videos should be taken on school devices and should only be saved on the school media drive.

Staff should ask for the consent of a child, using age-appropriate vocabulary, before taking their photo.

Use of Personal ICT

Use of personal ICT equipment is at the discretion of the school. Any such use requires the explicit permission of the Head teacher.

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).

The Senior Leadership team undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about 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.

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

Class Dojo

Class Dojo is a secure online site that allow schools to create portfolios for individual children and connect with parents.

Use of Class Dojo

All children and parents should be connected to Class Dojo. Staff can use these platforms to share images of children's work, events that have taken place in school, homework and any other suitable information.

If children do not have permission for their photo to be shared online, then their photos shouldn't be shared on the Class Story (Class Dojo).

Parents can use the messaging feature to contact their child's class teacher during the agreed hours (8am-5pm). Staff can reply to messages between these times but should log out of the app after 5pm.

The school does not expect staff to respond in writing on ClassDojo to significant issues that are raised through the platform. Parents are expected to speak directly to the class teacher, or to arrange a meeting with the relevant member of staff via the school office.

Staff may use ClassDojo on their personal phones, but are expected to log out when they leave school and log back in when they arrive at school.

Staff should report any inappropriate use by parents or children to the Leadership team immediately.

Remote Teaching

Zoom will be used by staff as the primary teaching platform to deliver live lessons during periods of school closure.

Only Class Dojo will be used as learning platforms to provide children with information to support their learning and to set and receive assignments.

All staff will adhere to the expectations set out in the safeguarding policy and below:

- All sessions will be conducted in a suitable location and ideally against a neutral background.
- Staff will teach remotely in groups or as a whole class. In some circumstances children feel anxious and a 1:1 session may be offered however we advise that an adult stays in the child's room.
- Language should always be professional, and suitable clothing must be worn.
- If a member of staff is sharing a screen, they must ensure all tabs they have open are appropriate for a child to see.
- Staff will be aware of specific functions and how to enable and disable them e.g. blocking chat and muting
- Lessons to be kept to a reasonable amount of time to ensure families are still able to continue with daily routines.
- Staff will use the classteacher@ when communicating with parents not their individual email accounts. When contacting parents by phone they will use 141 before the number to ensure their number is blocked.

Remote learning

If children are required to be taught remotely live lessons through the platform Zoom, parents will be sent rules for expectations and behaviour, and these will be discussed with the children at the first session. These include:

- All family members to wear suitable clothing and use appropriate language.

- Children should be out of bed and ready to learn just like they would in school.

- Children should demonstrate a good learning behaviour which includes not using the chat function during the lesson or using a mobile phone unless it is to access Zoom.