




Type of Document: **Policy**
Number of pages: 18
Date of adoption: September 2023
Date of Review: September 2024

Online Safety and Acceptable use Policy 2023-2024

Signed by Headteacher 

Signed by Chair  _____

Date:



UNCRC Article 13 - Children have the right to get and to share information.
UNCRC Article 17 - Children have the right to reliable information from the mass media.



Milton Mount Primary School E-safety policy

1. 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 a way that 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-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 scam

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance 'Keeping Children Safe in Education' and the 'Education for a Connected World' guidance.

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.

3. Roles and Responsibilities

3.1 Online safety team

Milton Mount has an Online Safety Team responsible for the implementation of this policy. Members include: DSL team representative; PSHE Lead; Computing Lead, online-safety co-Ordinator.

The Team work cohesively to implement online safety practise across the school and report regularly to the online-safety Governor.

3.2 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.

Within the DSL Team, the Online Safety Lead is Amanda Duda (Assistant Headteacher & SENCO). Working as part of the online safety team, the online safety 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 governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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 governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive

3.3 The governing body

The governing board implementation has overall responsibility for monitoring this policy and holding the headteacher to account for its.

The governing board will make sure all staff undergo 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 governing board 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 governing board 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 governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- 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.

The governor who oversees online safety is Richard Bundy.

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

3.4 The headteacher

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

3.2 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 DSLs 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

3.3 Parents

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](#)

4. Acceptable use of the internet 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 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 in order 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.

5. 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.

6. 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

7. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters in communications home via Studybugs and Class Dojo. 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 DSLs.

8. 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 either 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.

9. 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.

10. 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.

10. Cyber- bullying

10.1 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.

10.2 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 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:

- Children will miss 3 lunchtime playtimes in Giant Redwood
- The teacher and parents will be informed
- A letter will be sent to parents from the Leadership team
- 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 DSLs 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.

10.3 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 that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or a member of the DSL team,
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident 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](#)

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

11. Social networking

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.

Individual teaching staff that use a Twitter account for school should ensure that their tweets are in-line with the school policy and any photographs taken of school children, using their personal phones or cameras, are removed from these devices routinely.

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.

12. 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.

13. 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 has to 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 as long as the use complies with all other points of this policy.

14. 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.

15. 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.

16. 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.

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

The DSL 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 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..

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

18. Class Dojo

18.1 Definition

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

18.2 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-6pm). Staff can reply to messages between these times but should log out of the app after 6pm.

Staff can have these apps on their personal phones but they have 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.



UNCRC Article 13 - Children have the right to get and to share information.
UNCRC Article 17 - Children have the right to reliable information from the mass media.





Staff Acceptable Use Policy
issued by the Governors of Milton Mount Primary School



Effective from: September 2023

Signed by: Lesley King

Next review date: September 2024

The Staff Acceptable Use Policy reflects the UN Convention on The Rights of the Child (CRC) by supporting these Articles:

Article 3: The best interests of the child must be a top priority in all things that affect children

Article 16: Every child has the right to privacy

School networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or Academy Trust you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or Trust into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Head Teacher or a member of the Leadership team.

Use of phones and email

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s). All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of

confidentiality or breach of contract. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, they must inform the SBM immediately and follow our data breach procedure.

Staff are permitted to on occasion use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head teacher may withdraw or restrict this permission at any time and at their discretion.

Personal use of ICT facilities and the use of personal mobile phone is permitted provided that such use:

- Does not take place during teaching time/contact time
- Does not breach the acceptable use agreement
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Personal ICT use outside of school

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Network Security

Users are expected to inform the Head Teacher or a member of the Leadership team immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by a person authorised by the Head Teacher. Users identified as a security risk will be denied access to the network.

Media Publications

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work may only be published (e.g. photographs, videos, TV presentations, web pages etc.) if written parental consent has been given

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or Greensand Academy Trust) into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden. I will not access, create, store, link or send material that is offensive, obscene, pornographic or otherwise inappropriate.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to past or present students.
6	I will not trespass into other users' files or folders. This includes attempting to gain access to password-protected information without permission from authorised personnel.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Head Teacher or a member of the Leadership team.
9	I will ensure that I log off after my network session has finished and I will not allow or enable others to gain, or attempt to gain, unauthorized access to the school's ICT facilities.
10	If I find an unattended machine logged on under other users usernames I will not continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the Head Teacher or a member of the Leadership team. Any photos taken with permission on a mobile device will be deleted once uploaded which will be witnessed by either JSPC or Leadership Team
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.

14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Head Teacher or a member of the Leadership team.
15	I will not use "USB drives", portable hard-drives, tablets or personal laptops on the network without having them "approved" by the school and checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as school parents and their children.
19	I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role in any way.
20	I will support and promote the school's online safety and Data protection policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates the Data Protection Act or breaching the security this act requires for personal data, including data held in SIMS.
22	I will not receive, send or publish material that violates copyright law or breaches intellectual property rights. This includes materials sent/received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet (or taken offsite in any other way) will be encrypted or otherwise secured.

Declaration of understanding and compliance

As a school user of the network resources I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Head Teacher or a member of the Leadership team.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, 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 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.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name:

Staff Signature (if appropriate):

Date: __/__/____

During the updating of this policy, Safeguarding was taken account of.

Approved by the Governing Body