

MANSTON PRIMARY SCHOOL



ONLINE SAFETY POLICY

Manston Primary is committed to safeguarding and promoting the well-being of all children and expects our staff and volunteers to share this commitment.

Policy reviewed by: James Clay and Kirsty Thorpe

Approved by: Teaching, Learning and Pupil Support Committee

Date: September 2026 Review Date: September 2027



1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Maintain a culture of vigilance that protects pupils from online and offline harm arising from emerging technologies, digital platforms, and artificial intelligence (AI).

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) 2026, and should be read alongside Working Together to Safeguard Children (2026), the school's Safeguarding and Child Protection Policy and current local safeguarding procedures.

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#) – remove if not applicable, see section 4]
- [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.

3. Roles and responsibilities

3.1 The governing board

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

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), on induction, 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 body will ensure that the school has robust IT filtering and monitoring systems in place and should be informed in part, by the risk assessment required by the Prevent Duty in order to limit children's exposure to online risks. The governing body should consider the number and age range of children, those who are potentially at greater risk of harm and how often they access the IT system.

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 the 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.

At Manston we:

- use key stroke monitoring through classroom cloud software for all devices.
- The key word library used by classroom cloud is editable and appropriate to the age and number of pupils in school and their use of school devices both in and out of school.
 - This system is monitored by the Designated Safeguarding Lead and the ICT Co-ordinator.
- School uses Schools Broadband internet filtering to block key word searches for all uses (student and staff profiles both in place can be edited)

The governor who oversees online safety under their safeguarding remit. The current safeguarding governor is: Darren Scotland.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- 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

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and 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 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 (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
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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.

3.4 The ICT manager

The ICT manager Karen Cartwright is responsible for:

- Putting in place and managing an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis during child protection supervision between the DSL and deputy
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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 by reporting immediately to James Clay and or Karen Cartwright. This needs to be reported verbally and then followed up in an email.
- Following the correct procedures by reporting to the DSL will help the school to identify 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 and recorded on CPOMS under Behaviour and then either Cyberbullying or Online Behaviour
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the school's Home-School Agreement and pupil Acceptable Use expectations (Appendix 4).

Parents/carers 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](#)
- Parent resource sheet – [Childnet](#)

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

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

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

Primary schools insert:

In **Key Stage (KS) 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 (KS) 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)

Online safety is taught progressively through the school's PSHE/RSHE and computing curriculum. The Kapow Primary curriculum explicitly teaches online safety in line with the Education for a Connected World framework, including digital citizenship, cyberbullying, critical consumption of online information and misinformation, and safe online relationships. Learning is reinforced through assemblies, Safer Internet focus activity and responsive teaching when emerging risks are identified.

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

Teaching will reflect current and emerging online risks, including harmful content, online exploitation, artificial intelligence, misinformation, changes in how children communicate, and the impact of technology on relationships and wellbeing.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
 - Classroom cloud – monitoring
 - Schools Broadband – Lightspeed filtering
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

Details of our online safety curriculum and the key content for each year group can be found on our school [web site](#).

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school 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 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.

The 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. Class teachers will discuss cyber-bullying with their classes.

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

All staff, governors 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).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school 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 contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, the Deputy Headteacher and the Safeguarding and Welfare Officer 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 necessary senior personnel.
- 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, or if there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, the school's safeguarding policies and procedures will be followed, as detailed within the school's Safeguarding and Child Protection Policy.

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 any adult in school is made aware of an incident involving the consensual or non-consensual sharing of nude or semi-nude images/videos, including imagery created or altered using digital or AI tools, they must report it to the DSL immediately. Staff should recognise that such incidents may involve coercion, exploitation, bullying, sexual harassment or abuse. Staff must not:

- View, copy, print, share, store or save the imagery, or ask a pupil to share or download it. If imagery has been viewed accidentally, this must be reported to the DSL.
- Delete the imagery or ask the pupil to delete it.
- Share information about the incident beyond those who need to know, or say or do anything that may blame or shame a child involved.
- Ask pupils involved to disclose details about the imagery beyond what is necessary to establish an immediate safeguarding concern; further enquiries are the DSL's responsibility.

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](#)
- Our behaviour policy and behaviour addendum, which includes additional information on searches and confiscations

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are widespread and increasingly embedded in digital platforms. The school recognises both their potential educational value and the safeguarding risks that can arise from AI-generated or manipulated content, misinformation, impersonation and changes in how children access information and communicate online.

AI can be used to facilitate bullying, harassment and sexual harm, including through deepfakes or other synthetic images, audio or video that appear real. Any AI-generated or AI-altered nude or semi-nude imagery involving a child will be treated as a safeguarding concern and managed under the school's safeguarding procedures.

Misuse of AI that harms another pupil or member of staff, disrupts school discipline, creates a safeguarding concern or otherwise breaches school expectations will be managed in line with the Behaviour Policy, Safeguarding and Child Protection Policy and Acceptable Use agreements.

Staff will consider safeguarding, data protection, age-appropriateness and educational purpose before introducing new AI tools. Where a new AI tool is used by the school, an appropriate risk assessment will be completed and use will be in line with the school's Acceptable Use expectations.

7. Acceptable use of the internet in school

All staff will read this policy, and the school's acceptable use policy on CPOMS, and will 'mark as read' to evidence that they will adhere to all contents and stipulations stated in both policies.

Pupils will be expected to adhere to acceptable use of internet both in school, and on school devices at home, as stated in the school's home-school agreement.

Other stakeholders [parents/carers/volunteers/visitors] and governors are expected to adhere to the acceptable use policy and the school's ICT systems to ensure safe and appropriate internet use (appendices 1 to 3).

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 will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Manston Primary School is a mobile phone-free school during the school day. Only pupils in Years 5 and 6 who walk to and from school independently may bring a mobile phone, unless an exceptional individual arrangement has been agreed. Phones must be switched off before pupils enter the school grounds, handed to the class teacher immediately on arrival, stored securely for the school day and returned at home time. Phones are brought at the owner's risk.

Pupils must not use mobile phones, smart watches, earbuds or other personal electronic devices during lessons, break times or lunchtimes unless use is explicitly directed and directly supervised by a member of staff. Parents/carers must not contact pupils directly on personal devices during the school day; urgent communication should be made through the school office. Any device used in breach of these expectations may be confiscated and, following repeated or serious misuse, returned only to a parent/carer. Serious misuse, including cyberbullying or child-on-child abuse facilitated through digital communication, will be treated as both a behaviour and safeguarding matter.

Staff should only use their mobile phones at appropriate times of the day only e.g. break times. Normally, during the school day their mobiles should be turned off or set to silent.

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

Within EYFS, pupils do not have access to personal mobile phones or other personal electronic devices with imaging or sharing capabilities during the school day. Where exceptional use of technology is required, school-owned or school-managed devices are prioritised and use is directly supervised.

9. Using work devices outside school

All staff members, and those stakeholders borrowing school devices, will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Children and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- Staff and children must ensure terminals or laptops are locked, logged off (or hibernated) or turned off when left unattended. Offsite, all staff laptops must be fully shut down when unattended to activate the Bitlocker encryption system upon reopening/restarting again.
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ICT Manager, Karen Cartwright, or James Clay, Headteacher and DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

School sanctions may also be applied to online behaviour outside school where it harms another pupil or member of staff, impacts school discipline, damages the reputation of the school or creates a safeguarding concern.

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 safer working practice guidance. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, 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 up the risks
- 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 and Safeguarding and Welfare Officer 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

Online safety, cyberbullying and related safeguarding/behaviour incidents are recorded on CPOMS and reviewed through the school's regular safeguarding and behaviour monitoring. Relevant trends, including outcomes for vulnerable pupils, are considered by leaders and reported to governors as appropriate. Urgent concerns are acted on immediately.

This policy will be reviewed every year by the Headteacher and Safeguarding and Welfare Officer. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Phones in School Policy Addendums
- Home-School Agreement
- Personal Development Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

14. Appendices

- Appendix 1 - Pupil AUP
- Appendix 2 - Staff AUP
- Appendix 3 - Governor AUP
- Appendix 4 - Home-School Agreement

Pupils Acceptable Use Agreement

Respectful Communication:

- Use only respectful language online and avoid sending negative messages.

Personal Information:

- Keep all personal information private and never share passwords.

Careful Clicking:

- Always be careful when clicking on links or downloading files and check with an adult first.

Educational Use:

- School accounts, emails, TTRs, and other digital tools and equipment are strictly for educational purposes and will only be used by the assigned pupil. Follow the rules set by your teachers.

Reporting Issues:

- If something online makes you feel uncomfortable, immediately tell an adult.

Digital Responsibility:

- Your online actions are permanent, so act in a way that you can be proud of.

No Cyberbullying

- Cyberbullying is unacceptable. Report it if you experience or see it.

Image Sharing:

- Get permission before posting or sharing images and videos.

Positive Online Presence:

- Act responsibly online and be a positive influence.

Monitoring:

- The school monitors technology use to ensure safety and compliance.

Sanctions for Misuse:

- Misusing technology may lead to consequences, including discussing the issue at home, and in serious cases, informing future schools.



Staff and Volunteer Acceptable Use of Internet and Digital Technologies **Policy Staff Agreement**

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. Staff and volunteers agree to this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

All staff/volunteers agree to the following

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to obtain permission for children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people. (pupils names shown in pictures)
- I have read the procedures or incidents of misuse in the Internet and Digital Technology Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person in accordance with procedures listed in the Acceptable Use Policy.
- I know who the Designated Safeguarding Officers are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail.
- I know I should use the school e-mail address and phones to contact parents and other members of staff.
- I know to copy in the Head Teacher into any email to a pupil and for any emails to parents that they need to be made aware of.
- I know that I must not use the school system for personal use unless this has been agreed by the Head Teacher.
- I know that I should notify the school ICT lead/technician to perform a virus check on my laptop and other storage devices that I wish to use so that I do not inadvertently transfer viruses especially where I have downloaded resources. If I am unsure, I must not do anything and notify the ICT lead/Datacable immediately.

- I will ensure that I follow the Data Protection Act 2018 and UK GDPR and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Head Teacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden.
- I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been shown a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

Acceptable Use of Internet and Digital Technologies Policy

Children and parents agree that

- Users are responsible for good behaviour and following the school values on the Internet just as they are on school premises. General school rules apply.
- The Internet is used within school to conduct research, access educational material and communicate with others.
- The permission of parents/carers is required for pupil use of school devices outside of school. Parents/carers are responsible for any loaned devices and must immediately inform school of any issues or problems.
- Staff may review files and communications to ensure that users are accessing the system responsibly.
- Users should not expect that files stored on school equipment, servers or the school network would always be private.
- During school, teachers will guide children towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, movies, radio and other potentially offensive media.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks

- Violating copyright laws
- Using other users' passwords or passing password information onto others
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use in school and use of any school managed programmes outside of school.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

For Staff: By reading this document, and 'marking as read' on CPOMS, I am agreeing to understanding and implementing all of the contents within this policy and recognise that there will be sanctions should I violate any of these statements.

Volunteers and other adults to sign the below:

I have read and understood and agree to comply with the school's Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:

Manston 



Governors Acceptable Use of Internet and Digital Technologies Policy Agreement

Governors have a duty to ensure that the school and its staff, including themselves, are aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. All governors must agree to this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

1. I understand that 'digital' includes networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, smart watches, digital cameras, email and social media sites.
2. School owned information systems including TEAMS, must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by Manston Primary School can only be used by members of staff and governors and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware or to add anyone from outside of the school community to the school TEAMS account without permission from the system manager.
6. I will ensure that any school data or reports (that mention or contain information about or could identify pupils, staff or parents/carers) are kept in accordance with the Data Protection Act 2018 and UK GDPR. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
7. I will not keep or access documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted.
8. I will not store any personal information on the school system that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will respect copyright and intellectual property rights.
10. I will report all incidents of concern regarding digital safety to the Designated Safeguarding Lead (James Clay), his deputy (Kirsty Thorpe) and/or the ICT Manager (Karen Cartwright) as

soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to James Clay and or Kirsty Thorpe in his absence.

11. I will not attempt to bypass any filtering and/or security systems put in place by the school.
12. My electronic communications with staff, parents/carers will take place within clear and explicit boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels- TEAMS, phone call from school office and not via personal devices or communication channels e.g. social networking or mobile phones.
13. I will ensure that my online reputation and my use of digital and information systems are compatible with my role.
14. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
15. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the ICT Manager or the Head Teacher.
16. I understand that my use of the information systems, Internet and email on school systems may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Governor Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:

The logo for Manston, featuring the word "Manston" in a blue, cursive-style font. A blue swoosh underline extends from the end of the word, ending in a small yellow star.

Manston Primary Home-School Agreement



At Manston Primary, we firmly believe that our pupils become the best versions of themselves when school and home work in partnership. The development of a positive, respectful relationship between home and school is a crucial factor in every pupil's wellbeing and progress.

This Home-School Agreement sets out the shared expectations for the school, parents/carers, and pupils. By choosing to send your child to Manston Primary, you agree to uphold the expectations outlined below and support your child in doing the same.

Our School Rules

We do as we are asked

We treat everyone with kindness and respect

We have kind hands and feet

We always do our best

Manston Primary Home-School Agreement



- Treat all pupils, parents, carers, visitors, and staff members with kindness and respect
- Provide a safe, happy, inclusive environment where children are valued, listened to, and supported
- Deliver high-quality teaching and an engaging curriculum that meets the needs of all pupils
- Promote and uphold British values: democracy, the rule of law, individual liberty, and mutual respect for all faiths and beliefs
- Provide the support children need to achieve their full potential
- Share pupils' progress regularly through books, reports, parent meetings, and the Arbor App
- Provide home learning opportunities including reading, phonics, and online tools like TTRS and Numbots
- Model and support restorative approaches to behaviour, promoting reflection, responsibility, and repair
- Respect confidentiality and communicate in a clear, open, and timely manner
- Keep the school website, newsletter (Sway), and Arbor App updated with relevant policies, events, and information
- Provide guidance to parents on how to use the Arbor App to monitor attendance, report absences, access reports, update details, and receive communications
-

- Treat all pupils, staff, and members of the school community with kindness and respect
- Ensure my child attends school regularly and arrives on time in the correct uniform or PE kit
- Report absences to school, ideally using the Arbor App, and keep the school updated on health and contact details
- Communicate respectfully and calmly with school staff, modelling positive behaviour for my child
- Refer to the Home-School Communication Policy for how and when staff will respond (acknowledgement may take up to 3 school days)
- Use the Arbor App to:
 - View attendance, Report absences, Update contact information, Access reports & Make payments
- Support home learning by encouraging completion of:
 - Weekly homework tasks (booklets or paper sheets)
 - Reading
 - Times Tables Rock Stars (TTRS) and Numbots
 - Weekly phonics activities (for younger pupils)
- Support the school's restorative behaviour approach by discussing issues calmly with my child and helping them reflect on and resolve concerns
- Attend parent meetings and follow through on any agreed actions or support plans
- Regularly read the school's newsletter, check the calendar and Arbor messages
- Refer to the School Communication Policy for further information on working together to support my child's learning and wellbeing

As a pupil I will:

- Follow our school rules:
 - We have kind hands and feet
 - We do as we are asked

Manston Primary Home-School Agreement



- We treat everyone with kindness and respect
- We always do our best
- Come to school on time, wear the correct uniform or PE kit, and stay clean and tidy
- Be responsible for my learning and my actions, both in school and at home
- Bring in my reading book, homework, and letters when needed
- Complete all home learning tasks and practise regularly (reading, TTRS, Numbots, phonics)
- Respect the school environment and take care of equipment, books, and property
- Use technology responsibly and follow the Acceptable Use Policy
- Reflect on my behaviour and choices, and learn from all experiences
- Tell a trusted adult if I am worried or unhappy

*British Values at Manston Primary: Democracy, The rule of law, Individual liberty and Mutual respect for all faiths and beliefs

Manston Primary Home-School Agreement



Pupils Acceptable Use Agreement

Respectful Communication:

Use only respectful language online and avoid sending negative messages.

Personal Information:

Keep all personal information private and never share passwords.

Careful Clicking:

Always be careful when clicking on links or downloading files and check with an adult first.

Educational Use:

School accounts, emails, TTRS, and other digital tools and equipment are strictly for educational purposes and will only be used by the assigned pupil. Follow the rules set by your teachers.

Reporting Issues:

If something online makes you feel uncomfortable, immediately tell an adult.

Digital Responsibility:

Your online actions are permanent, so act in a way that you can be proud of.

No Cyberbullying

Cyberbullying is unacceptable. Report it if you experience or see it.

Image Sharing:

Get permission before posting or sharing images and videos.

Positive Online Presence:

Act responsibly online and be a positive influence.

Monitoring:

The school monitors technology use to ensure safety and compliance.

Sanctions for Misuse:

Misusing technology may lead to consequences, including discussing the issue at home, and in serious cases, informing future schools.