

Online safety policy

Morden Primary School



Approved by:	Teaching and Learning Committee	Date: 4.10.23
Last reviewed on:	20/09/2023	
Next review due by:	20/09/2024	

Contents

1. Aims	2
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating pupils about online safety	5
5. Educating parents/carers about online safety.....	6
6. Cyber-bullying.....	7
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school	9
10. How the school will respond to issues of misuse.....	9
11. Training	9
12. Monitoring arrangements.....	10
13. Links with other policies.....	10
Appendix 1: KS1 acceptable use agreement.....	11
Appendix 2: KS2 acceptable use agreement.....	12
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	14
Appendix 4: acceptable use agreement (parents).....	16
Appendix 5: online safety training needs – self-audit for staff.....	18
Appendix 6: Documentation.	19

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

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](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [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), 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.

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 (appendix 3)
- 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

Details of the school's designated safeguarding lead (DSL) and deputy/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 (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
- › 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 IT manager

The IT manager is responsible for:

- › Putting in place 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 monthly basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files in collaboration with the SLT (senior leadership team) and DSL/DDS

- › 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 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- › 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 filling out the relevant report form available on the school's extranet (Staff Portal).
- › If a site that is currently blocked is needed for educational purposes a request form must be submitted to the IT manager using the relevant form available on the extranet.
- › Working with the DSL to ensure 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 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'

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 terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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 International](#)
- › Parent resource sheet – [Childnet International](#)

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 (appendix 3).

4. Educating pupils about online safety

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

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

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) whom they do not know

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

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

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters 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
- › 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.

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.

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, 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 and/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 and/or DSL/DDSL
- › 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, the severity of that material will dictate the response. This will range from sanctions outlined within our behaviour policy, escalating to parental contact and finally contacting the relevant authorities.

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/Headteacher immediately, who will contact the appropriate authorities. The DSL/Headteacher 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.

6.4 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.

Morden Primary 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.

Morden Primary will treat any use of AI to bully pupils in line with our anti bullying and behaviour policies.

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 on the school's network.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We 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

Pupils in year 6 are permitted to bring mobile devices into school when walking home alone at the end of the day. These devices should be switched off when in school and kept in the school office. Children should collect these devices at the end of the day and not turn them on until outside the school building.

Any child caught using a non-school issued mobile device during school hours will have the device confiscated and will be asked to collect it at the end of the school day from the school office. Repeat offenders may be refused permission to bring mobile devices onto the school grounds and have their permission to walk home alone revoked.

9. Staff using work devices outside school

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

- Make sure that their password is secure. It is recommended to all staff that their password should be a minimum of 8 characters long and involve a combination of upper and lower case, numbers and special characters.
- The device is intended for work use only and should not be used by anyone other than the staff member who signed for it.
- Allow all security updates to run as soon as possible this included anti-virus and anti-malware programs.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the I.T Manager.

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 behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents 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, 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/DDSL 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

At Morden Primary we use Impero classroom monitoring software which is capable of viewing all computer and laptop screens connected to our network in real time.

Any inappropriate material that is not picked up by our filtering will be logged and reported to the IT manager.

All safeguarding and behaviour issues relating to online safety will be recorded on our CPOMs online management system.

As technology evolves and new risks are identified the IT manager along with the SLT and DSL/DDSL will review and adapt this policy to help protect the school community.

13. Links with other policies



This online safety policy is linked to our:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff code of conduct
- › Data protection policy and privacy notices
- › Complaints procedure
- › AUP (acceptable use policies) examples below.

Appendix 1: KS1 acceptable use agreement

Please note there is a pictorial AUP for those who need it. This is available on request. However, children in EYFS will receive this automatically.

My name is _____

1. I will only **USE** the devices and applications I'm asked to.
2. I will **ASK** for help if I'm stuck or not sure; I **TELL** an adult if I'm upset, worried, scared or confused.
3. I care for my **FRIENDS** and will tell someone if I think they need help
4. If I am **WORRIED** about anything, I can talk to an adult
5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE**
6. Anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS**  unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must especially online.
9. I always check before **SHARING** my personal information or other people's stories and photos.
10. I am **KIND** and polite to everyone on and offline

Adults I can talk to include:

_____ at school
_____ at home

Signed _____



SafeguardED

Draw yourself

Appendix 2: KS2 acceptable use agreement

As you grow you will be given more responsibility and this is the same for using devices at Morden Primary School. Throughout your time in KS2 you will have the opportunity to explore a wide range of technology, applications and projects. It is expected that you will follow the guidelines below not only within the school grounds, but when using devices at home too.

1. **I treat people with respect** – On or offline, everyone deserves to be treated respectfully.
2. **I ask permission** – At home or school, I only use the devices, apps, sites and games I have been allowed by my trusted adults.
3. **I respect others and their work** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
4. **I don't share my passwords** – I keep my login information for devices and applications to myself. I only share with my trusted adults at home and school.
5. **I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
6. **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. **If I make a mistake** – I will be honest and tell an adult so they can help me fix it. Mistakes are evidence that you are learning.
8. **I will only communicate online IF...** – It is with people I know in real life, a trusted adult knows and has given permission or when collaborating with others at school.
9. **I understand that everything online may not be as it seems** – I know that others online may not always be who they claim to be and information on websites may not be 100% accurate. I will always talk to a trusted adult if I am not sure.
10. **My body is private!** – I never share parts of my body that are under my clothes when using a device with a camera. NO ONE should make you do anything you are not comfortable with and if they do you NEED to **tell an adult immediately**.
11. **I say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
12. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
13. **I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it). Future employers will be able to check my digital footprint.
14. **I follow the rules even if someone says I don't have to** – I know that apps and websites have age limits for a reason. I understand that by using these apps and sites when I'm not meant to is potentially putting myself at risk of receiving inappropriate content and/or harm.
15. **I respect people's work** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
16. **Social media** – I understand that social media accounts usually require users to be 13 years old or older. I know I should not have social media accounts while at primary school and if I am found to have them the school may report my account to the relevant vendor and my parents.

17. **Using school technology** – I understand that all devices in school are monitored and I should only use approved applications. By downloading or using applications that have not been approved I understand that my account may be suspended.
18. **I will not pretend to be someone else** – It is not OK to pretend to be someone else online for any reason. To do this breaks rule number 1! I understand that my account will be suspended and reported to the vendor of the application in question as well as my parents. In extreme cases the police or other authorities may be involved.
19. **I will not take photos of other people without their consent** – I understand that taking photos of others without their consent can lead to them feeling unhappy or worried about where the image may be displayed or used.

~~~~~

**I have read and understood this agreement. If I have any questions, I will speak to a trusted adult at school or at home.**

**Please give two examples of your trusted adults 1 at home and 1 at school.**

1) \_\_\_\_\_ at home. 2) \_\_\_\_\_ at school

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_



**SafeguardED**

## Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

### Background

We ask everyone involved in the life of Morden Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and all adults that use our equipment, internet connection and online resources are asked to sign it when starting at the school and whenever changes are made. All adults within the school community even for a short visit agree to uphold the values of our Online Safety policy.

Outlined below are the minimum of what is expected and is not an exhaustive list. We expect all adults in the Morden community to act as role models to our children.

If you have any questions about this AUP or our approach to online safety, please speak to the DSL/DDSL or IT Manager

### What am I agreeing to?

1. I have read and understood Morden Primary's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to keep up to date through CPD actioned by the school where appropriate.
3. All concerns relating to children's use of technology and online content must be reported to the DSL/DDSL immediately. Any concerns relating to adult use of technology or online content should be reported to the headteacher, if the concern relates to the headteacher than the chair of governors should be notified.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language. For more information on the RAFT approach to language we use please see our behaviour policy.
7. When/if overseeing the use of technology by children in school I will make sure I am aware of all the tools available to help me effectively monitor the children in my care. I know I can contact the IT Manager at any time for help and advice using Microsoft Teams. If the IT manager is not contactable, I know I can seek assistance from the DSL/DDSL.
8. When preparing materials, for class and/or display, that includes online content, I will take due care and diligence to ensure that the content is safe and respectful and that the content does not include any inappropriate adverts and/or images. It is understood that changes can happen without your knowledge, but any incident involving inappropriate content being consumed (intentionally or unintentionally) by children will be reported using the staff portal form or reporting to the DSL/DDSL.
9. I understand that all school devices are installed with monitoring software that means the school can monitor usage on or offsite. School devices remain the property of the school and are loaned for the purpose of school business only. You should not use these devices for any personal endeavours. Any concerns voiced or notifications received from the monitoring software will be investigated and this could lead to disciplinary action in accordance with the code of conduct policy.

10. I am aware of the filtering systems used within school and the types of content blocked. I am aware of the increased focus within KCSIE 2023, and that filtering is now led by the DSL. I am aware that any breaches of filtering should be reported via the staff portal or to the DSL/DDSL immediately and if I feel we are blocking a genuine educational resource I can submit a request form for the unblocking of this content via the staff portal and/or the DSL/DDSL.
11. I understand that as an adult in Morden Primary school I am a role model to others within the school community. I will conduct myself in accordance with the staff handbook, code of conduct and will demonstrate safe, respectful and mature use of all online interaction. As an employee of the school, I am an ambassador for the school's ethos and values thus should consider this when using engaging in online public discussions and sharing of content in the public domain.
12. I will only use school approved methods for contacting members of the school community. I will never use my own personal email, messaging or social media channels to communicate with parents and children of the school community. If you are contacted outside of approved channels, you should not reply and should report this to the Headteacher at the earliest opportunity.
13. I will adhere to the schools Data Protection policy at all times. No information from the network or MIS should be shared without permission from the DSL/DDSL/Headteacher. Exceptions to this include safeguarding requests from authorised parties such as LADO, MASH, social services, police etc if you have ANY doubt, please seek confirmation from DSL/DDSL/Headteacher before sharing.
14. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

### To be completed by the user

I confirm I have read and understood this acceptable use policy. If you require any clarification on any of these points please speak to the DSL/DDSL or the IT manager.

**Signature:**

\_\_\_\_\_

**Name:**

\_\_\_\_\_

**Role:**

\_\_\_\_\_

**Date:**

\_\_\_\_\_



**SafeguardED**

## Appendix 4: acceptable use agreement (parents)

### Background

We ask everyone involved in the life of Morden Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Outlined below are the minimum of what is expected and is not an exhaustive list. We expect all adults in the Morden community to act as role models to our children.

If you have any questions about this AUP or our approach to online safety, please speak to the DSL/DDSL or IT Manager

### Where can I find out more?

You can read Morden Primary's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to the DSL (Designated Safeguard Lead) or IT manager by contacting the school office and arranging an appointment.

### What am I agreeing to?

1. I understand that Morden Primary uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that use of school configured devices, school internet connectivity, networks and cloud platforms out of school are subject to filtering and/or monitoring.
5. I understand that my child may require assistance when accessing home learning material online and I will do my best. Support is available by emailing [homelearning@morden.merton.sch.uk](mailto:homelearning@morden.merton.sch.uk) for help logging on and accessing home learning material.
6. I understand my child may contact and be contacted via emails sent through Google Workspace, our approved method of contact outside school. Children are encouraged to report any communication received through Google Workspace that they do not recognise.
7. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
8. Parents are kindly asked not to call pupils on their mobile phones during the school day as we require any children bringing in such devices to have them turned off and locked in the school office; urgent messages can be passed via the school office by calling 020 8648 4168.
9. I will do my utmost to make sure my child follows age limits when online. Nearly all social media accounts require users to be 13 years or older. We understand that occasionally children may gain access to these accounts, but ask that you support the school by monitoring and preferably closing these accounts when discovered.



10. I understand that not all members of the Morden Primary community will have the same opinions as myself regarding sharing and posting images online. I will therefore only take photos of my child at any school event. Images taken that have other children in focus should not be used online.
11. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and can refer to [parentsafe.lgfl.net](https://parentsafe.lgfl.net) or <https://www.nspcc.org.uk/keeping-children-safe> amongst others for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...
12. I understand that whilst home networks are much less secure than school ones, I have the option to apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games advice can be found [parentsafe.lgfl.net](https://parentsafe.lgfl.net). There are also child-safe search engines for example swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
13. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen on the school website, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

For more information, please read our online safety policy which can be found on our school website or by contacting the school office.

~~~~~

By choosing to send your child/ren to Morden Primary School you automatically agree to the above in principle. You understand that children are integrated into a society where online consumption is almost mandatory for life. We encourage you to:

PLAY – WATCH – LEARN
with your child online.

Let's encourage a world full of safe, responsible and creative learners that will foster a much kinder and more inclusive online and offline community.



Appendix 5: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Who is the DSL?	
Please give 2 examples of inappropriate content that children might be able access at school?	1. 2.
If a child reports that inappropriate content or something has made them feel uncomfortable, what do you need to do?	
Where can you find the Online Safety policy?	
Are you familiar with the school's acceptable use agreement for pupils?	
<p>STAFF ONLY – Are you familiar with the filtering and monitoring applications used within Morden Primary?</p> <p>▶ Filtering looks at web traffic and attempts to stop content that shouldn't be displayed from being displayed on devices.</p> <p>▶ Monitoring is software that can see what is happening on a connected device.</p>	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: Documentation.

All behaviour records and incidents relating to children within Morden Primary school are documented on CPOMs.

Separate to this we document all filtering exclusions and explicitly allowed sites. We record the reason as to why we as a school have chosen to block or allow the content for our pupils.

URL	Allow	Block	Reason
/y8.com			Gaming site - Games not suitable
1001games			Gaming site - Games not suitable
animixplay.to			Animai viewing deemed unsuitable for children

We have deployed an online form to report filtering incidents which can be filled in via our staff portal. Visitors and those without access to the portal can report incidents to the DSL/DDSL. There is also a form located on the staff portal where staff can request access to currently blocked sites.

* Required

1. Name *

Enter your answer

2. Which key stage is this for? *

EYFS

KS1

KS2

3. URL - Please supply the full website address. *

Enter your answer

4. Please state your reason for wanting this site unblocked. *

Enter your answer

All requests are discussed with SLT (senior leadership team) and the

DSL/DDSL within school. If it is decided that the resource is unblocked than our IT manager will administer the change to the filtering.