



Online Safety Policy

Reviewed
Summer 2025

Marshgate Primary School

Online Safety Policy

INTRODUCTION

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless or smart technology. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

Marshgate Primary School's Online Safety Policy will operate in conjunction with other policies including those for Behaviour and Relationships (including anti-bullying), Computing, GDPR and Child Protection & Safeguarding.

As outlined in the Computing Policy, online safety forms an integral part of the curriculum and is taught within all units of Computing. It is also included in PSHE and other subjects and the school provides additional education on online safety through assemblies, parent/carers meetings and communications.

AIMS / APPROACH

Our aims for the delivery of online safety are the following:

- To ensure robust processes are in place to ensure the online safety of pupils, staff, volunteers and governors.
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of the internet and other digital technologies - including mobile and smart technology.
- To ensure pupils develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world. This includes displaying a sense of responsibility and respect to themselves and others while online.
- To identify and support groups of pupils that are potentially at greater risk of harm online than others.
- To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

FOUR 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

Marshgate Primary School

Online Safety Policy

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

LEGAL DUTIES AND RESPONSIBILITIES

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on the following:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for Head Teachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying, 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.

Our school is registered with the Data Protection Commissioner's office to protect personal data; however individuals have a right of access to personal educational data belonging to them. Please see GDPR Policy.

We use London Grid For Learning (LGFL) as the school's Internet Service provider.

They provide the following services:

- Facility for multiple access.
- Filtering from the less desirable elements of the internet.
- The filtering of junk mail.
- The ability to configure internet access i.e. to limit access to news groups, chat rooms, personal email.
- E-mail addresses.

Virus protection software as recommended by PFI provider / Nexus will be installed on all school systems.

All teachers are familiar with the Pupil's Code of Practice for the use of the internet. The use of online resources should always be supervised and the Code of Practice adhered to.

Marshgate Primary School

Online Safety Policy

All staff are familiar with and adhere to the Teachers' Code of Practice for safer internet use.

The Obscene Publications Act 1959 and 1964 makes it an offence to have an obscene article for publication or gain (publication includes distribution, circulating, selling, hiring, giving or lending, showing, playing or projecting). Disciplinary action will be taken in the event of teachers using the internet inappropriately.

If pupils either deliberately or accidentally access or download unsuitable materials, the following procedure should be followed:

1. The screen should be turned off (but the device should not be).
2. Any mobile devices or printed materials should be confiscated.
3. In line with safeguarding procedures, the Designated Safeguarding Lead (DSL) should be informed immediately. The pupil's access to the internet should be suspended until the DSL has investigated further.
4. Refer to the Behaviour and Relationships Policy for any further action.

The Nexus technician will audit internet linked computers on a regular basis to ensure that no inappropriate files have been downloaded.

All internet activity should be appropriate to staff professional activity or pupil's education, however, the occasional personal use by staff is permitted.

As this is a rapidly changing area, this Online Safety policy is subject to frequent monitoring and review.

All staff are trained in Safeguarding procedures, including elements of online safety and The Prevent Duty.

ROLES AND RESPONSIBILITIES

1. The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety.

2. The Head Teacher

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

3. The Designated Safeguarding Lead

Details of the school's DSL [and deputy/deputies] are set out in the school's Child Protection and Safeguarding Policy as well as relevant job descriptions. The school's DSL is the Head Teacher.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with governing board to review this policy 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

Marshgate Primary School

Online Safety Policy

- Working with the Computing Lead and IT Provider (Nexus) to make sure the appropriate systems and processes are in place
- Working with staff and IT Provider (Nexus), 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 and Relationships policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the 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.

4. The Computing Subject Lead & IT Provider (Nexus)

The computing subject leader and IT Provider (Nexus) are responsible for liaising with the Head Teacher / DSL to ensure:

Appropriate filtering and monitoring systems are in place to ensure pupils are safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

Access to potentially dangerous sites is blocked and, where possible, the downloading of potentially dangerous files are prevented.

Any online safety incidents that are reported to the Computing Lead or that are noticed by Nexus are passed on immediately to the Head Teacher / DSL.

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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.

Working with the Head Teacher / DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and that of the Behaviour and Relationships Policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour and Relationships Policy

6. Parents

Parents are expected to:

Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

Marshgate Primary School

Online Safety Policy

What are the issues? - [UK Safer Internet Centre](#)

Hot topics - [Childnet International](#)

Parent factsheet - [Childnet International](#)

7. Visitors and Members of the Community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

CURRICULUM

1. Linked with the computing curriculum.

As outlined in the Computing Policy, pupils in Key stage 1 are taught to:

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- 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

In Key stage 2, Pupils are taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Marshgate Primary School

Online Safety Policy

2. Linked with the PSHE curriculum.

Relationships and sex education (RSE) and health education will be taught in PSHE lessons. This includes learning:

- 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

3. Online Safety Curriculum

From Spring 2022 children have been taught online safety using 'Project Evolve' created by the UK Safer Internet Centre in partnership with SWGfL. Online safety is broken down into 8 key areas that children will focus on across the year:

1. Self-Image and Identity
Shaping online identities and how media impacts on gender and stereotypes.
2. Online Relationships
Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
3. Online Reputation
Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.
4. Online Bullying
Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation.
5. Managing Online Information
Strategies for effective searching, critical evaluation and ethical publishing.
6. Health, Well-being and Lifestyle
The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by

Marshgate Primary School

Online Safety Policy

online technologies and the strategies for dealing with them.

7. Privacy and Security

Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

8. Copyright and Ownership

Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

EDUCATING PARENTS ABOUT ONLINE SAFETY

The school will raise parents' awareness of online safety where appropriate through parentmail or other communications, and in information via our website. This policy will also be made available on the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher.

INTERNET ACCESS AND FILTERING

As outlined in the Computing Policy, teachers must supervise pupils and take all responsible measures to ensure that children access only appropriate material. Internet access in the school is provided by LGFL, who provide a service designed for pupils, which includes filtering appropriate to the age of the pupils.

Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

REMOTE LEARNING FROM HOME

Children are only directed towards approved home learning platforms – e.g. Education City, MyMaths and Timestables Rockstars.

Seesaw and Google Classroom are accessed by children and used to organise and complete some school work and homework (with oversight and supervision from parents when at home). The children use logins set-up by the school and / or through LGFL. Where children are directed towards links, teachers must ensure they have been checked and all possible measures taken to assess the suitability of the resource and how it links to the intended learning objective.

COVID PROCEDURES

Permission for teachers to set-up 'Google Meet' and video conferencing with children is temporarily granted for a limited time while schools are closed. This is at a set time approved by the HT and with parents/carers informed in advance. All 'Google Meets' are always with more than one pupil.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy and where appropriate referrals

Marshgate Primary School

Online Safety Policy

made to children's social care by the DSL. Online teaching should follow the same principles as set out in the school code of conduct.

Marshgate will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when using online learning platforms or delivering virtual lessons, especially where webcams are involved:

As per the additional staff protocol for online learning, provided to all staff, professional conduct should always follow requirements as when in school (the school's staff code of conduct and the staff internet code of practice).

- No 1:1s with children, group "meets" only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers (staff and pupils) used should be in appropriate areas where possible, for example, not in bedrooms.
- Live classes should be kept to a reasonable length of time
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms agreed by Marshgate: Google meet video conferencing.
- Staff should record, the length, time, date and attendance of any sessions held.
- Staff should follow up non-attendance with parents via phone call and emails

NETWORK SECURITY

No users may change or modify the hardware, network wiring or software configurations. The IT technicians (Nexus) are the only personnel with the network administration rights.

CYBER-BULLYING

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

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. It will be discussed in class and the issue will be addressed in assemblies.

Marshgate Primary School

Online Safety Policy

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE 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.

The school also sends information/leaflets on cyber-bullying to parents so that 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 and Relationships 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. Sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying and behaviour procedures. Please see Behaviour and Relationships Policy and Safeguarding and Child Protection Policy for more information.

EXAMINING ELECTRONIC DEVICES

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils and staff are expected to adhere to the Online Safety code of practice. All internet activity should be appropriate to staff professional activity or pupil's education, however, the occasional personal use by staff is permitted.

Marshgate Primary School

Online Safety Policy

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. A guest wi-fi account has been created and can be given to trusted professionals while on-site but only to assist with professional activity i.e Governor Meetings, Speech and Language Meetings or Educational Psychologist Reviews.

Websites visited by pupils, staff, volunteers, governors and visitors are monitored (where relevant) to ensure they comply with the above.

STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. A work device or USB device containing school data should not be left in an unattended car at any point.

If staff have any concerns over the security of their device, they must seek advice from the IT Providers (Nexus) and the Computing Subject Lead. Work devices must be used solely for work activities.

HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

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

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

E-MAIL POLICY

All teachers must adhere to the following conditions of use.

1. Appropriate language should be used for all on-line communications.
2. E-mails should not be used to create, use, transmit or encourage material which is:
 - Pornographic, inappropriate or unsuitable
 - Illegal, obscene or libellous
 - Offensive or annoying
 - Defamatory
 - Violates another person's privacy

Marshgate Primary School

Online Safety Policy

3. E-mail should not be used for gambling, advertising or soliciting for personal gain or profit.
4. Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
5. Posting anonymous messages and forwarding 'chain' communications is forbidden.
6. Users should not sign up to any information services which send you regular information via e-mail unless this is directly related to school activities.
7. Users should not transmit any material in violation of any British laws. These include the Data Protection Act, Computer Misuse Act and Design Copyright and Patents Act.
8. Users should not use e-mail for product advertisement, commercial activities or political campaigning unless authorised to do so by the school.
9. Users should log off properly from networks after use to ensure that other users do not have unauthorised access.
10. Staff should adhere to the in-school policy and agreement of not sending emails at the weekend, and before 6am or after 6pm on working days.

Pupils, being taught about e-mails and their safe use may only use approved e-mail accounts on the school system – namely those supplied by LGFL.

As part of using emails safely, pupils are taught to immediately tell a teacher if they receive offensive material. They are also taught to never reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

During lessons, whole class or group e-mail addresses are used supplied by LGFL with access to external personal e-mail accounts permanently blocked.

SOCIAL NETWORKING

All social networking sites are blocked. They are not used by pupils in school. Use by adults is only when a specific use is approved (eg. PSA Twitter feed).

Pupils are taught how to use social networking safely using specifically designed educational packages. This includes never giving out personal details of any kind which may identify them or their location when using social networking outside of school. Pupils are also advised / taught about the posting of appropriate images and pictures.

Pupils are taught internet communication good practice including security and how to set 'strong' passwords, deny access to unknown individuals and what to do when they receive unwanted communications. Pupils are also taught to invite known friends only and deny access to others.

Marshgate Primary School

Online Safety Policy

MOBILE PHONE POLICY

Mobile phones should not be used on school premises (this includes watches that can access the internet, make calls, take photos or record audio / videos). Year 5 and Year 6 children may bring mobile phones or smart watches to school, but they must be deposited with the teacher prior to the start of lessons and collected at the end of the day. A safe space has been allocated inside the school gates for children to check mobile phones before leaving the school site to walk home by themselves (walking permission lists detail individual pupil arrangements for those to whom this applies). Staff are only permitted to use mobile phones (including smart watches) in line with the school staff mobile phone policy.

ARTIFICIAL INTELLIGENCE (AI)

This section of the Online Safety Policy has been updated in line with the DfE Policy Paper - Generative Artificial Intelligence (AI) in Education, 10th June 2025.

The school acknowledges the growing presence and influence of generative artificial intelligence (AI) technologies, such as ChatGPT, Google Bard, and other AI-driven content creation tools. These technologies are increasingly accessible to staff, pupils, and parents/carers.

AI has the potential to enhance teaching and learning through:

- Personalised support and resources for pupils.
- Time-saving planning tools for staff.
- Opportunities to explore digital literacy, ethics, and responsible technology use.

When used appropriately, AI can support curriculum delivery and pupil engagement. However, its use must be carefully managed to ensure it aligns with safeguarding, data protection, and teaching standards.

Risks and Concerns

AI tools also present significant risks, including:

- Misinformation: AI-generated content may be inaccurate or misleading.
- Bias and discrimination: Outputs may reflect biased training data.
- Data privacy: Inputting personal or sensitive data may breach GDPR.
- Bullying or harm: AI-generated content, including deepfakes or fake messages, may be used to harass or embarrass pupils or staff.

Expectations for Staff

At all times, Staff must comply with the wider statutory obligations as stated in Keeping Children Safe in Education and Child Protection and Safeguarding documents. Staff must not input confidential or identifiable pupil or staff data into AI tools. Staff must carry out a risk assessment before introducing new AI tools for classroom or professional use. AI should not replace professional judgment or critical thinking in planning, marking, or communication.

Marshgate Primary School

Online Safety Policy

Staff are encouraged to engage in regular training on the ethical and safe use of AI in education.

Expectations for Pupils

Pupils should be taught how to critically assess AI-generated content.

Use of AI tools must follow the school's online safety code of practice.

Misuse of AI to create harmful or deceptive content will be treated as a serious breach of school rules and safeguarding policy.

POLICY ON THE CREATION OF THE SCHOOL WEBSITE

The following protocol for creating or adding to the website should be followed:

1. All links within pages, including links to external sites, should be fully tested and working and should be tested to ensure that no unsuitable material can be accessed.
2. Any e-mail should be cleared with the people involved and written permission obtained.
3. All articles, pictures or icons which are from 'third party' must have copyright clearance in writing.
4. Photographs of children, which could be misused, should not be put on web pages. Photographs, which are of distant shots or group shots may be used providing permission from parents is given prior to use. Blurred or back views are also acceptable. (Parents are requested to sign a Marshgate Primary photography consent form, which is then held in the school office).
5. Pages created should be of high quality without spelling/syntax errors of fact.
6. Pages should link to the home page.
7. Where 'last updated' dates are used these should be current.
8. The policy is that no individual is named except by prior agreement.
9. The school's site should include a contact and address for the school but references to other identifiable individuals are covered by the Data Protection Act.
10. The school is registered under the Data Protection Act.
11. Users should not use the school's website for general advertisement, commercial activities or political campaigning.

We buy in to the services of a website designer:

- to keep our website up to date and attractive
- to interact with the wider community

Marshgate Primary School

Online Safety Policy

- to be able to update information quickly and effectively

Teachers updating class pages should have regular training and be aware of the policy regarding the school website.

THE PREVENT DUTY AND ONLINE SAFETY

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Our staff receive regular training and are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the wellbeing of any pupil is being compromised.

REVIEW

As this is a rapidly changing area, this Online Safety Policy is subject to frequent monitoring and review.

Marshgate Primary School

Online Safety Policy

MARSHGATE PRIMARY SCHOOL PUPILS' ONLINE SAFETY CODE OF PRACTICE

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parent/carer.
- I will never give my password to anyone; even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parent/teacher/carer and get them to come to the first meeting.
- I will never 'hang around' in an internet chat room if someone says or writes something which makes me feel uncomfortable or worried and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or social media posts and I will always report it to a teacher or a parent.
- I will not look for bad language or distasteful images while I'm on-line and I will report bad language or distasteful images to a teacher or a parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the internet provider will check the sites I have visited.
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the internet if I deliberately misuse it or the school's systems.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the teacher and Computing Technicians.
- I may not download software from the internet (including screen savers, games, video clips, audio clips, *.exe files)
- I know that information on the internet may not always be reliable and sources may need checking.
- I will not use e-mail to send or encourage material which is illegal, offensive or annoying or invades another person's privacy.

If required to be signed and dated, the detail below can be included.

Pupil's name: _____

School: _____

I have read the Pupil's Code of Practice and I have discussed it with my child.
We agree to support the school's policy on the use of the Internet.

Signed: _____ (Parent/Guardian/Carer)

Pupil: _____

Marshgate Primary School

Online Safety Policy

MARSHGATE PRIMARY SCHOOL STAFF ONLINE SAFETY CODE OF PRACTICE

- Teaching staff should closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages.
- Computer monitor screens should be readily visible for the teacher, so they can monitor what the pupil is accessing.
- Pupils should have clear guidelines for the content of e-mail messages, sending and receiving procedures.
- Use of the internet by pupils should be supervised by a teacher or adult.
- Pupils should be taught skills and techniques to enable efficient, effective and safe use of the internet.
- Pupils should have a clearly defined focus for using the internet and e-mail.
- If offensive materials are found the monitor should be switched off (but the device itself should not be), any printed materials confiscated and offensive URLs given to the DSL.
- Virus protection has been provided by the school as viruses can be downloaded accidentally from the internet. Teachers should be aware that pupils bringing work from home on USB sticks, could also infect the computer.
- The recommended ISP will regularly check sites visited by schools (all pupils and staff).
- It is recommended that pupils do not use open forums such as newsgroups or chat rooms.
- Disciplinary action may be taken if the internet is used inappropriately by staff e.g. for accessing pornographic, racist or offensive material or for personal financial gain, gambling, political purposes or advertising (this includes creating, sharing, linking to or sending such material).
- The internet should not be used by staff in any way which could harm the school's reputation.
- No access is permitted by staff through the school IT systems to social networking sites or chat rooms.
- No improper language should be used by staff when communicating online, including in emails or other messaging services (see e-mail policy)
- Staff are not permitted to install any unauthorised software, or connect unauthorised hardware or devices to the school's network without permission.
- Staff should not share passwords with others or log in to the school's network using someone else's details.
- Photographs of pupils should not be taken without checking with teachers first.
- Staff should not share confidential information about the school, its pupils or staff.
- Staff should not access, modify or share data they're not authorised to access, modify or share.
- No staff should promote private businesses, unless that business is directly related to the school.
- All reasonable steps should be taken to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I have read the Internet Code of Practice for pupils and teachers and I am familiar with the school's Online Safety and Computing Policies including e-mail, web site creation, remote learning from home and mobile phone policies.

If required to be signed and dated, the detail below can be included.

I agree to abide by these policies and the staff's Internet Code of Practice.

Name: _____

Signed: _____

Marshgate Primary School

Online Safety Policy

Date: _____