MARSHSIDE PRIMARY SCHOOL

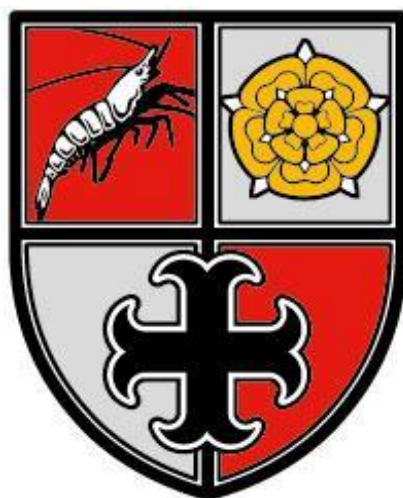**E-Safety Policy**
September 2023

Date Approved by Full Governing Body: 19.9.23

Chair: Andrew Brown

Headteacher: Natasha Sandland

Review Date: September 2024

EQUALITY STATEMENT

Our school recognises children's diverse circumstances and is committed to its legal responsibilities under the Equality Act 2010. Each child regardless of their background could be a victim of child abuse and is therefore entitled to the same degree of protection and support.

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

Aims, scope and principles

The use of the Internet as a tool to develop learning, understanding and communication has become an integral part of school and home life. In using any form of communication within the public domain there is risk therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children and staff use these technologies.

Marshside Primary School will endeavour to safeguard against all risks through a robust and proactive E-Safety Policy. Any incidents that may arise will be dealt with quickly and according to our policy to ensure students continue to be protected.

Purpose:

The purpose of this document is to ensure that all users of Marshside Primary School's ICT (Information Communications Technology) Services and the internet feel confident and safe in the use of ICT and the internet in pursuit of their job and studies, and understand their roles and responsibilities in relation to appropriate use of ICT and the internet.

Aims:

The aim of this policy document is to describe what is acceptable activity and use of Marshside Primary School's ICT network, internet and equipment to protect the disclosure of information and ensure we can prevent, as far as possible, cyber-attack or cybercrime and exposure to inappropriate or harmful content.

Marshside Primary School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Governors

- Have robust Filtering and Monitoring Systems to provide a safe environment to learn and work, including when online.

- 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 roles, responsibilities and strategies to deliver and maintain effective filtering and monitoring systems to identify, intervene and escalate an incident, where appropriate

We expect that all teachers will act in accordance with the personal and professional behaviours set out in the Teachers' Standards.

We expect all support staff, governors and volunteers to also act with personal and professional integrity, respecting the safety and wellbeing of others.

We expect everyone to understand and behave in accordance with our HEART values.

Failure to follow the E-Safety Policy may result in disciplinary action being taken, as set out in our staff disciplinary procedures.

Please note that this E-Safety Policy is not exhaustive. If situations arise that are not covered by this code, staff will use their professional judgement and act in the best interests of the school and its pupils.
This policy refers to and complements other policies and guidance at Marshside including:
- ICT Acceptable Use Policy
- Safeguarding and Child Protection Policy
- SEN Policy
- Whistleblowing Policy

Legislation and guidance

Keeping Children Safe in Education 2023

Scope

This document applies to all authorised users of Marshside Primary School's ICT systems; including teaching and support staff, non-teaching staff, supply teachers / assistants, students, governors, volunteers, contractors, consultants, visitors (e.g trainers), commissioned service providers and organisations that connect to or support any part of the IT Infrastructure.

Individual Responsibilities

The Governing Body

The Governing Body has had due regard to the additional information and support set out in KCSiE and ensures that the school has a whole- school approach to online safety and a clear policy on use of communications technology in school.

The Governing Body has overall strategic responsibility for filtering and monitoring and will review annually that the standards are being met. (KCSiE 2023)

Our Safeguarding Governor is: Jo Swift

Senior Leadership Team

The headteacher is responsible for procuring filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of provision and overseeing reports.

They are also responsible for making sure that all staff understand their role, are appropriately trained, follow policies, processes and procedures, act on reports and concerns.

The ICT Network Manager

Apex Network Solutions Limited are contracted to manage the school's network.

They are responsible for:

• Ensure that appropriate filtering and monitoring systems are in place to safeguard children and young people

from potentially harmful and inappropriate online material. The use of filters is routinely monitored and updated any breaches dealt with in accordance with school procedures;

Be careful to ensure that these systems do not place unreasonable restrictions on internet access or limit what children can be taught with regards to online teaching and safeguarding;

• Whilst filtering and monitoring is an important part of schools' online safety responsibilities, it is only one part of our role. Children and adults may have access to systems external to the school control, such as mobile phones and other internet enabled devices and technology. Staff are required to adhere to the Acceptable Use Policy and the Code of Conduct. Children will hand in any devices to the school office at the beginning of the day and will collect at the end of the day.

• 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 weekly basis.

• 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 and are logged on the CPOMs system.

• Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

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, ensuring that pupils follow the school's terms on acceptable use; **r**eporting and recording any incidents of cyber-bullying or exposure to unsuitable material and that they are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

Parents

Parents 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 (appendix 1)

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 and Acceptable Use Policy when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in via Class Dojo, letters or other communications home. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, this can be raised with any member of staff, the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised the Headteacher.

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 intentional harming of one person or group by another person or group, either one-off or repetitive, where the relationship involves an imbalance of power.