St. Mary's

MULLYMESKER

eSafety Policy

This policy is based on and complies with DENI Circular 2013/25 on eSafety and Acceptable Use Policy guidelines, which highlights schools' responsibility to have in place an eSafety policy ***and*** *an Acceptable Use Policy (AUP).*

1. Introduction

In St Mary's Primary School we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

This eSafety policy sets out measures taken by St Mary's Primary School to 'mitigate risk through reasonable planning and actions' (DENI, 2013, 2.2) in areas of internet technology and other electronic communication mediums such as mobile phones, games consoles and wireless technology.
The policy has been drawn up by the staff of the school under the leadership of the Principal & ICT coordinator.
It has been approved by governors and circulated to all parents.
The policy and its implementation will be reviewed regularly.

2. What is eSafety?

eSafety is electronic safety. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. eSafety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

In relation to St Mary's Primary School, eSafety is;

- concerned with safeguarding our pupils in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Our eSafety policy operates in conjunction with our other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use (AUP). eSafety is planned for and delivered as part of the curriculum in our school as part of Using ICT across the curriculum.

3. Professional Development of Teaching Staff at St Mary's;

Teachers are the first line of defence in eSafety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity. As part of our eSafety, staff will have the opportunity to avail of access to training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection or the member of Senior Management with responsibility for eSafety. Staff are also informed and provided with additional support and advice from C2k, Social Services or the PSNI if required.

4. Education of Pupils

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. Two of the main resources for education children at St Mary's Primary School if the importance of eSafety are;

Child Exploitation and Online Protection (CEOP) which explains how to be SMART online, and;

Childnet International. This is a non-profit organisation working to "help make the Internet a great and safe place for pupils". Our schools uses many of the Childnet-produced materials to support the teaching of eSafety at Key Stage One and Two. We also use these materials to inform parents, staff and governors.

5. Cyber Bullying

Staff at St Mary's are aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This

form of bullying is addressed within our school's overall anti -bullying policy and pastoral services as well as this eSafety policy.
Social media is rarely used for teaching and learning, also children are educated about the risks and issues related to social media. Each of the social media technologies can offer much our school and pupils but each brings its own unique issues and concerns and as such when considering using a social media platform staff to discuss this with the eSafety coordinator.

Cyber Bullying can take many different forms and guises including:

- *Email* – nasty or abusive emails which may include viruses or inappropriate content.
- *Instant Messaging (IM) and Chat Rooms* – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- *Social Networking Sites* – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- *Online Gaming* – abuse or harassment of someone using online multi-player gaming sites.
- *Mobile Phones* – examples can include abusive texts, video or photo messages.
- *Abusing Personal Information* – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following legislation covers different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
- Malicious Communications (NI) Order 1988
- The Communications Act 2003

At St Mary's Primary School, pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.
Cyber-bullying incidents are monitored and recorded by the eSafety coordinator.

6. Email security

C2k recommend that all staff and pupils should be encouraged to use their C2k email system. They also advise that staff should not use home email accounts for school business.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

7. Internet security

Staff and pupils accessing the Internet via the C2k Education Network are required to authenticate using their C2k username and password. This authentication provides Internet filtering via the C2k Education Network solution for the protection of staff and pupils alike.

Policy agreed with Principal, ICT Co-ordinator, whole staff and Board of Governors - June 2015.