St Mary’s Primary School Granemore

Internet Safety Policy

Rationale

Now that the internet has become an integral part of the fibre of today’s society, we in St Mary’s, believe that it is incumbent on all members of staff to actively support safe and responsible behaviour when using any forms of technology.

Whether children are surfing the web, adding to blogs, commenting, gaming or posting on social media, we all share a collective responsibility to ensure that children are empowered to act in their own best interests and in the interests of everyone else.

Scope of the Policy

This policy applies to all members of the school (including staff, students, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The following section outlines the internet safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Internet Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about internet safety incidents and monitoring reports.

Child Protection Team

The Child Protection Team has a duty of care for ensuring the safety (including internet safety) of all members of the school community. All in the Child Protection Team should be aware of the procedures to be followed in the event of a serious internet safety allegation being made against a member of staff.

Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

* They have an up to date awareness of internet safety matters and of the current internet safety policy and practices (shared through staff meetings and child protection training)
* They have read, understood and signed the staff Code of Conduct
* They report any suspected misuse or problem to the Head Teacher for investigation/action/ sanction
* All digital communications should be on a professional level and only carried out using official school systems
* Internet safety issues are embedded in all aspects of the curriculum and other activities Pupils understand and follow the internet safety and acceptable use policy (Appendix 3)
* Pupils have a good understanding of research skills and how to access safe sites.
* Staff monitor the use of digital technologies, mobile devices and cameras in lessons and other school activities.
* In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through information leaflets, parents’ evenings (linking up with local club where appropriate), newsletters, letters, website and information about national/local internet safety campaigns. Parents and carers will be encouraged to support the school in promoting good internet safety practice and to follow guidelines.

Some parents and carers need support to fully develop their knowledge of the internet safety risks and issues affecting their children. They play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in internet safety is therefore an essential part of the school’s internet safety provision. Children and young people need the help and support of the school to recognise and avoid internet safety risks and build their resilience.

Internet safety should be a focus in all areas of the curriculum and staff should reinforce internet safety messages across the curriculum. The internet safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• An internet safety curriculum should be provided as part of Computing/PDMU/other lessons and should be regularly revisited.

• Key internet safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities

• Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. This is enhanced by the Securus facility which compels children to buy into using computers properly

• Staff should act as good role models in their use of digital technologies, the internet and mobile devices

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches, and where possible Apple Classroom may be used.

• Where pupils are allowed to search the internet (age appropriate), staff should be vigilant in monitoring the content of the websites the young people visit.

Technical – Infrastructure / Equipment, Filtering and Monitoring

Through the C2k System, all children and staff are offered a level of security. It is, however, recognised that Google search results cannot be filtered. Where a member of the school community is able to access inappropriate content, ICT coordinator (E Magee) should be informed and steps will be taken to block that website.

Since our school has a full set of iPads, these should be used with caution. The children have the facility to record and to take photos and videos. The children need to be made aware that these should only be used as part of classroom learning and that all recordings should be deleted afterwards.

Bring Your Own Device (BYOD)

St Mary’s has the facility, through the C2k site to allow children to bring their own devices to school and to connect to our school’s network, however, since we have a full complement of iPads in the school, we do not encourage children to use anything that does not belong to the school.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Children need to be aware that that it is common for employers to carry out internet searches for information about potential and existing employees. The school will endeavour to educate our children of these risks:

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Parents/guardians are asked for permissions for taking images/videos and sharing them on different platforms. Plays and assemblies are treated individually and where there is an objection, no images will be taken.

• Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should **only** be taken on school equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Pupil’s work can only be published with the permission of the pupil and parents or carers.

### Points for Children to Consider

#### Follow These SMART TIPS

**S**

**Secret -** Always keep your name, address, mobile phone number and password private – it’s like giving out the keys to your home!

**M**

**Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent’s/carer’s permission, and then when they can be present.

**A**

**Accepting** e-mails or opening files from people you don’t really know or trust can get you into trouble – they may contain viruses or nasty messages.

**R**

**Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

**T**

**Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees

**An Acceptable Use of the Internet**

Children should know that they are responsible for making an Acceptable Use of the Internet.

They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Class\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* On the network, I will only use my own login username and password.
* I will not look at, change or delete other people’s work/files.
* I will ask permission before entering any website, unless my teacher has already approved that site.
* I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and sensible.
* When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
* I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
* If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
* I understand that if I deliberately break these rules I could be stopped from using the Internet.

Parental signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Points for** **Parents to Consider**

It is important to promote Internet Safety in the home and to monitor Internet use.

* Keep the computer in a communal area of the home.
* Ask children how the computer works.
* Monitor on-line time and be aware of excessive hours spent on the Internet.
* Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
* Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
* Discuss the fact that there are websites which are unsuitable.
* Discuss how children should respond to unsuitable materials or requests.
* Remind children never to give out personal information on the Internet.
* Remind children that people on line may not be who they say they are.
* Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
* Be aware that children may be using the Internet in places other than in their own home or at school.

# **Filtering for the Home Computer –**

Parents may wish to invest in security software for their children’s computers. Some of this software works by monitoring all Internet activity for trigger words.

There are many types of security software available.

Examples include:

* Net Nanny, [www.netnanny.com](http://www.netnanny.com)
* Surfwatch [www.safesurf.com](http://www.safesurf.com)

**Guidance Material on Internet Safety**

<http://schoolsl.becta.org.uk>

[www.ceop.gov.uk](http://www.ceop.gov.uk)

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

Examples of safety rules for children are also available from:

<http://www.kented.org.uk/ngfl/policy>