Girnhill Infant School

'Where everyone is valued and futures matter'

Online Safety Policy

The wider use of emerging technologies is important in order to enhance teaching and learning in schools. Access to the internet and a wide range of resources for learning are considered essential and plays a major role in any learner's development. Schools need to have good management processes in place to ensure safe and effective use of the Internet by staff, pupils and other stakeholders.

Introduction

Use of technologies within school and at home is continually expanding and has become an integral part of learning and communication. The Internet brings pupils into contact with a wider range of information, the scope and nature of which may or may not be appropriate for the pupil.

Using the Internet is now an everyday occurrence for most adults and children. With ever expanding new technologies such as blogs, social networking spaces, online chat and mobile phones to name a few children are using technology in a way never seen before. The increased use and reliance of technology at school and home also exposes children to a number of risks and dangers. In its simplest form-

Online Safety is about ensuring children use new technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

The schools Online Safety policy is part of the schools safeguarding policy and school aims to update it regularly in this ever-changing area.

The need for an Online Safety policy

There is evidence that the digital world is having an impact on the welfare of children and young people and those that work with them. There are related risks and these impact upon the school curriculum.

The Byron review - makes a case for "empowering young people to manage risks and make the digital world safer" and identifies on-line risks as being problematic because of their anonymity and ubiquity.

Curriculum

The statutory computing curriculum expects pupils to learn how to locate, retrieve and exchange information using Computing. When planning the curriculum, teachers need to prepare for and make use of computing and communications technology. Access to lifelong learning and enhancement of employment requires learners to be capable in the use of computing and there is a need to develop skills in their use.

Through the use of the Internet based activities those adults supporting learning within a school environment are able to enrich the range of opportunities and resources available to learners. They should be aware of the risks as well as the opportunities presented.

Within the Computing scheme of work are learning objectives related to esafeguarding. These skills are embedded within the teaching of computing and are clearly stated within planning, demonstrating progression. Online Safety is a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of computing across the curriculum.

In lessons processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.

Requests for unblocking a website can be made through Wakefield Councils EDIT Centre, these requests should be auditable, with clear reasons for the need.

Pupils should be taught in all lessons to be critically aware of the materials / content they access online 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

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of the Computing curriculum.
- This will cover both the use of computing and new technologies in school and outside school.
- Key Online Safety messages will be addressed through a planned programme of assemblies, newsletters and teaching.
- Pupils will 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 will be helped to understand the pupil acceptable use policy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Guidance on how to stay safe on line are displayed around school and in classrooms.
- Staff should be aware that they are role models in their use of computing, the internet and mobile devices.

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 Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Parents / Carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will inform parents / carers of any developments within the Online Safety policy and strive to send a positive message home about the safe use of technologies.

Parental meetings will take place to deliver the message of Online Safety in a meaningful way. They will be supported in delivering the message of On Line Safety at home and partnership work with West Yorkshire Police in school will support in this area through assemblies.

Training and Staff

A planned programme of formal e-safeguarding training will be made available to staff.
All new staff should receive e-safeguarding training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.
Online Safety policy and its updates will be presented to and discussed by staff in Teacher meetings and TA meetings, governor meetings.

All staff must sign and agree to the acceptable use policy before using any school computing resource.

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented in co-operation with Alamo (technical support).

School computing systems will be managed in ways that ensure that the school meets any esafeguarding technical requirements and Acceptable Usage Policy and any relevant Local Authority Online Safety policy and guidance.

There will be regular reviews and audits of Online Safety and security of school computing systems.
Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school computing systems. Details of the access rights available to groups of users will be recorded by the Network.
Usernames and password will be restricted for the use of the identified individuals only.
The administrator passwords for the school computing system, used by the Network Manager must also be available to the Headteacher and kept in a secure place.

Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that this is known to others.

Any filtering issues should be reported immediately to our technical support, Alamo.

Requests from staff for sites to be removed or added from the filtered feed will be considered by the Headteacher in school and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

Appropriate and relevant security measures are in place to protect the servers, firewalls, routers, wireless systems, hand held devices etc from accidental or malicious attempts, which might threaten the security of the school systems and data.

The school infrastructure and individual workstations are protected by up to date virus software. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Published content and the school website / Learning Platform

Staff or pupil personal contact information will not generally be published. The contact details given online are for the school office. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children will be used.

Pupils full names will not be used anywhere on a school web site or other on-line space in association with photographs.

Pupil age / work file names will not refer to the pupil by name.

Social networking and personal publishing

Within school children will not have access to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

School staff have signed an acceptable user policy and are aware of their professional responsibility when using social networking sites. Staff will not access social network sites using school equipment or during their working hours. Staff are aware that if they choose to access social networking sites during their own time no reference should be made about Girnhill Infant School.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Procedure for children / staff to report inappropriate content

A senior member of staff will deal with complaints of technological misuse.

Any complaint about staff misuse must be referred to the headteacher and the Whistleblowing Policy will be followed. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

This On Line Safety policy was last reviewed in September 2019 and will be reviewed annually.

This policy was reviewed in September and ratified by governors on 2nd October 2019.