"Living and Learning through Faith, Hope and Love"

WEETON ST MICHAEL'S C.E. PRIMARY SCHOOL

E-SAFETY & ACCEPTABLE USE POLICY

SEPTEMBER 2019

E-safety and acceptable use

1. Rationale - The Importance of Internet use in Primary Education

The Internet is universal with significant educational benefits resulting from appropriate curriculum Internet use as well as maintaining a digital dialogue with our parents, wider school family and community partners. This includes access to information from around the world and the abilities to communicate widely.

The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The following E-safety policy includes all digital devices and platforms, including all Internet-enabled hand-held devices.

All safe-guarding and child-protection guidelines expressed in this policy are pursuant to with the Keeping Children Safe in Education 2016.

Using the Internet in education allows:

Access to all age-appropriate world-wide educational resources.

Access to expert up to date knowledge for both pupils and staff

Fast communication links to support services, professional associations and colleagues;

Fast exchange of data with the LGfL and DfES.

Internet use will enhance learning because:

Use of the Internet will be built into Curriculum Planning for all subjects to specifically enrich and extend the learning process.

Staff will guide pupils in on-line activities that are planned to support the learning outcomes for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval; appraisal of bias and subjectivity and copyright materials.

2. Overview of Issues and Risks

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. ICT can offer many positive educational and social benefits to both adults and pupils, and both should be clearly educated on the benefits and risks involved when going online, including:

Copyright infringement - Copyright law applies on the Internet: staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Exposure to inappropriate materials - There is a risk that when using the Internet, young people may be exposed to material that is pornographic, hateful and violent in nature, encourages activities that are dangerous or illegal, is just age-inappropriate, biased or in contrast to Weeton St Michael's whole-school values. As a school we seek to build pupil's understanding and confidence in dealing with e-Safety issues, both at home and school.

Inappropriate or illegal behaviour - Online bullying is an unfortunate aspect of the use of Internet-enabled technologies. This can damage victim's self-esteem and pose a threat to their wellbeing. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

No access to chat-rooms, Instant Messaging services and bulletin boards.

Pupils are taught how to use the Internet safely and responsibly in line with our Child Protection and PSHEE policies and new Computing Curriculum (September 2014).

Physical danger and sexual abuse - Criminal minorities make use of the Internet to make contact with young people with the intention of establishing and developing relationships with young people with the sole purpose of persuading them into sexual activity. There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends. Inappropriate or illegal behaviour by school staff - This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent images. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities.

3. Principles of Internet Safety

The School Internet Policy is built on the following five core principles:

Guided educational use - Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. There is a clear distinction of learning about Computing & ICT and learning with computing & ICT.

Risk assessment – Use of the Internet poses certain risks to which our pupils are aware and able to act responsibly. We will ensure that everyone is fully aware of such risks, perform risk assessments and implement the policy for Internet use. Pupils need to know how to act and report inappropriate material.

E-safety and acceptable use

Responsibility - Internet safety depends on staff, schools, governors, advisers, parents and the pupils themselves taking responsibility for the use of Internet on all devices. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions will be judged carefully.

Regulation - The use of unsuitable resources, for instance un-moderated chat rooms or Instant messaging services present immediate dangers that are challenging to monitor and are therefore banned.

Appropriate strategies - This policy describes a number of strategies to help to ensure responsible and safe use. They include developing children's 'netiquette' in response to safe and responsible Internet use, developing responsibility and on guiding pupils towards educational activities. This requires staff, parents and pupils to be active participants and supporters of safe online activities

4. Creating a safe E-learning environment

The first challenge in creating a safe ICT learning environment is to ensure that everyone is aware of the issues and how they impact upon the school environment and the pupils. Awareness will be raised, in part, by a comprehensive Internet safety education programme for the whole school community. The programme will be continuous, responding to specific incidents and issues, and providing information about emerging technologies as well as those already embedded within the culture of the school. The Headteacher and staff will all be responsible for ensuring the promotion of a safe E-learning environment.

4.1 Roles and responsibilities

Internet Safety Lead

The primary responsibility of the Internet Safety Lead will be to establish and maintain a safe ICT learning environment within the school. Working with the other staff such as technician and the Headteacher to develop, or review, appropriate Internet safety policies and procedures.

Leading the development of management protocols so that any incidents in which Internet safety is breached are responded to in an appropriate and consistent manner, with the appropriate authority to take action as necessary.

Leading in the creation of a staff professional development programme that addresses both the benefits and risks of Internet-enabled technologies.

Leading in the creation of an Internet safety education programme for pupils, maintaining an overview of activities across the school, and supporting staff with information and resources as appropriate.

Developing a parental awareness programme.

Maintaining a log of all incidents relating to Internet safety in school.

Updating the governing body on current Internet safety issues, in conjunction with the Headteacher.

Liaising with outside agencies, which may include the LEA, local schools, or national agencies, as appropriate.

E-safety and acceptable use

Headteacher

Taking ultimate responsibility for Internet safety issues within the school, while delegating day-to-day responsibility to the Internet Safety Lead.

Supporting the Internet Safety Lead in creating an Internet safety culture within the school, including speaking to staff and pupils in support of the programme

Ensuring that the Governing body is informed of the issues and the policies

Ensuring that appropriate funding is allocated to support Internet safety activities throughout the school, for both the technical infrastructure and Inset training promoting Internet safety across the curriculum.

Governing body

The Governing body has statutory responsibilities for child protection and health and safety, and elements of these will include Internet safety. At Weeton St Michael's the main responsibilities related to E-safety are delegated to the Asset Management Committee

Developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the Headteacher and E-safety Lead in implementing these, including ensuring access to relevant training for all school staff

Promoting Internet safety to parents, and providing updates on Internet safety policies.

Teaching Staff and Volunteers

Develop and maintain knowledge of Internet safety issues, particularly with regard to how they might affect children and young people

Implementing school policies through effective classroom practice

Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the Internet Safety Lead in line with school Internet safety policies

Planning classroom use of the Internet and ICT facilities to ensure that Internet safety is not compromised; for example, evaluating websites in advance of classroom use and ensuring that school filtering levels provide appropriate protection for topics being studied

Embedding teaching of Internet safety messages within curriculum areas wherever possible

Maintaining an appropriate level of professional conduct in their own Internet use both within and outside school.

E-safety and acceptable use

Pupils

Upholding school policies relating to acceptable use of the Internet and other communications technologies

Developing their own set of safe and discriminating behaviours to guide them whenever they are online

Reporting any incidents of ICT misuse within school to a member of the teaching staff

Seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way

Communicating with their parents or carers about Internet safety issues, and upholding any rules for safe Internet use in the home

4.2 Technological tools

The school will work in partnership with the LEA to ensure systems are in place to protect pupils and that they are reviewed and improved.

An LEA filtering system is in place to minimise access to inappropriate content via the school network.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the LEA via the e-safety lead.

It will be possible to keep track of web pages visited and downloaded files to help investigate possible issues and monitor Internet usage.

4.3 Internet safety education programme for the whole school community

Pupils

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home however Internet and ICT literacy is unfortunately not synonymous with Internet and ICT safety.

The school will follow the Computing & ICT SoW as developed from new National Curriculum for Primary Schools (September 2014) – where age-appropriate information technology and digital fluency skills are embedded in the heart of the curriculum.

Safe-surfing messages should be reinforced every time pupils use the Internet and related technologies.

Instruction in responsible and safe use should precede Internet access.

'Rules of Internet use' will be posted near to computer systems. Pupils will be reminded of their acceptance of the rules and related consequences should the rules be breached.

Pupils will be informed that Internet use will be monitored.

E-safety and acceptable use

Pupils should be taught to be critically aware of the materials they read and know that material is not necessarily valid just because it is on the Internet.

Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Parents

Parents and carers also have a key role to play in creating a safe ICT learning environment and culture, through promoting Internet safety at home and hence reinforcing the messages taught in school. The children are taught to use the Internet sensibly and responsibly. It is recommended that parents also develop a similar set of rules if their children are using the Internet at home. In this way, we can promote responsible and safe Internet use at home and in school.

E-safety meetings for parents are arranged on a regular basis.

Parents' attention will be drawn to the School Internet Policy in newsletters, the school prospectus and on the school Web site.

Internet issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Sign-posting parents & carers to online support resources (See References & Resources)

4.4 E-mail Management

Pupil access to e-mail in the school is via Lancashire's E-mail management system only. Class e-mails are available and in certain supervised projects and lessons a pupil's individual account can be created. Pupil's individual accounts will only be available for the duration of the project and should not last for longer than one academic year, where passwords will be reset by the account manager.

Staff should not use school ICT facilities to access external personal e-mail accounts for business unrelated to their professional roles.

A responsible adult will supervise pupils when writing and sending e-mails and the content of outgoing and incoming e-mails should be checked by the adult (the class teacher whenever possible). This should lessen the risk of inappropriate materials being exchanged.

Children will be taught to never reveal personal details such as home addresses or telephone numbers during e-mail dialogue

Pupils will be taught to write polite and responsible e-mails.

The class teacher has responsibility to ensure that no abuse of the e-mail facility occurs

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

4.5 Newsgroups, Chat Rooms and Instant Messaging

Pupils will not be allowed access to public or unregulated chat rooms, newsgroups or instant messaging services.

4.6 Managing Internet use

Pupils are not permitted to use Mobile phones or other hand held devices in school. These are to be surrended at the main office and kept safe until hometime.

5. Web site content management

The school has a school website for the purpose of keeping parents informed about important, dates and events as well as providing information about the school and its related policies. Including images of pupils on the school website is crucial in celebrating success and promoting Weeton St Michael's whole-school values and pupil voice however the following non-negotiables must be adhered to:

Staff or pupils' home information will not be published.

Web site photographs that include pupils will be selected carefully

Pupils' full names will not be used anywhere on the Web site

Pupils will not be named under any photos in any digital communication from the School.

Image files will be appropriately named (pupils names not used in image file names) and are appropriately stored on the school's network.

The Headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.

The Web site should comply with the school's guidelines for publications.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

6. School Face book Site content and access management

Social media provides an instant and wide-reaching medium in which to engage a high volume of parents, carers and community partners. As such, the school operates a Face book Page account, adhering to similar guidelines as the schools' website.

Staff or pupils' home information will not be published.

Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.

Pupils' full names will not be used anywhere on the profile

Pupil's names will not be tagged or posted in any photos.

Image files will be appropriately named (pupils names not used in image file names) and are appropriately stored on the school's network.

Staff will be responsible for ensuring the appropriateness of any/all personal content shared.

Staff will be responsible for setting their own privacy settings.

The school will delete any inappropriate posts.

The school will ban any profiles from accounts known or suspected to belonging to pupils.

7. Safe and appropriate management of digital images

The school has given consideration to the way in which digital images including video are captured and stored within school for the protection of both pupils and staff. There are a number of internet-enabled hand held-devices with digital photography capabilities. Staff is made aware of the appropriateness of holding images on personal digital cameras and video. Pupils may also be involved in video conferencing activities where there is the possibility of images captured by a 3rd party.

Images will be taken and stored on school equipment only – as outlined in the school's Child Protection policy.

Images captured on digital devices will be transferred to the school server immediately (where practicable) and cleared off devices immediately (where practicable) – this is also to aid management of digital devices

If images are taken with personal equipment they should be transferred to the school network as soon as possible and deleted immediately.

Images of pupils or staff will not be captured or copied without permission and will not be stored at home without permission

All images and video where possible should be stored on the secure TEACHERS> PHOTOS shared drive area of the network and files clearly named for ease of archiving material.

8. Internet access authorisation

The school will keep a record of all staff, pupils and 3rd parties who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.

Parents will be informed that pupils will be provided with supervised Internet access.

Written permission from parents or carers will be obtained before any type of Internet access is allowed.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials such as the use of bookmarked sites or web quests, where pre-tested and approved sites only are accessible. This provides a good model for Internet access at lower Key Stage 2 although the range of sites available may increase.

E-safety and acceptable use

Pupils in may, under supervision, use search engines to carry out approved searches. Free Internet searching is highly discouraged – teachers should assess the potential risk before undertaking such activity.

Staff should not conduct free searches using classroom presentation equipment in full view of pupils. Projectors should be turned off whilst staff check suitability of search results.

Pupils may not use the Internet at any time without supervision. They should be reminded of the rules for Internet use at regular intervals.

9. Staff consultation

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.

Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

10. Responding to incidents of misuse

Minor incidents

Minor incidents of misuse by pupils might include; copying information into work and failing to acknowledge the source, downloading materials or images not relevant to their studies, and misconduct associated with pupils files, such as using someone else's password or deleting someone else's files.

In all cases the pupils will be issued with a warning and referred back to the rules of Internet use. The incident should be documented.

The Internet Safety Lead will monitor minor incidents to identify trends in pupils' behaviour, and will react to any emerging issues. This might include raising awareness on a particular Internet safety topic at a school assembly or offering staff additional training.

Incidents involving inappropriate materials or activities

Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network.

Serious incidents relating to Internet safety in schools will be reported to the Internet Safety Lead immediately. The Internet Safety Lead must document the incident and decide on an appropriate course of action, which will include involving the Headteacher and may also include external agencies. It may also be necessary to involve child protection

E-safety and acceptable use

Staff to provide follow-up counselling and support.

The Internet Safety Lead will review Internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.

If a child discovers something on the Internet that makes them feel uncomfortable or upset, they must report it immediately to their teacher. Pupils will be taught to turn off the monitor so that attention is not drawn to the material.

Although the Internet access at Weeton St Michael's is filtered in order to screen inappropriate sites, it may still contain inappropriate material. The site must be reported immediately to the Internet Safety Lead who will ensure that the website is flagged county-wide.

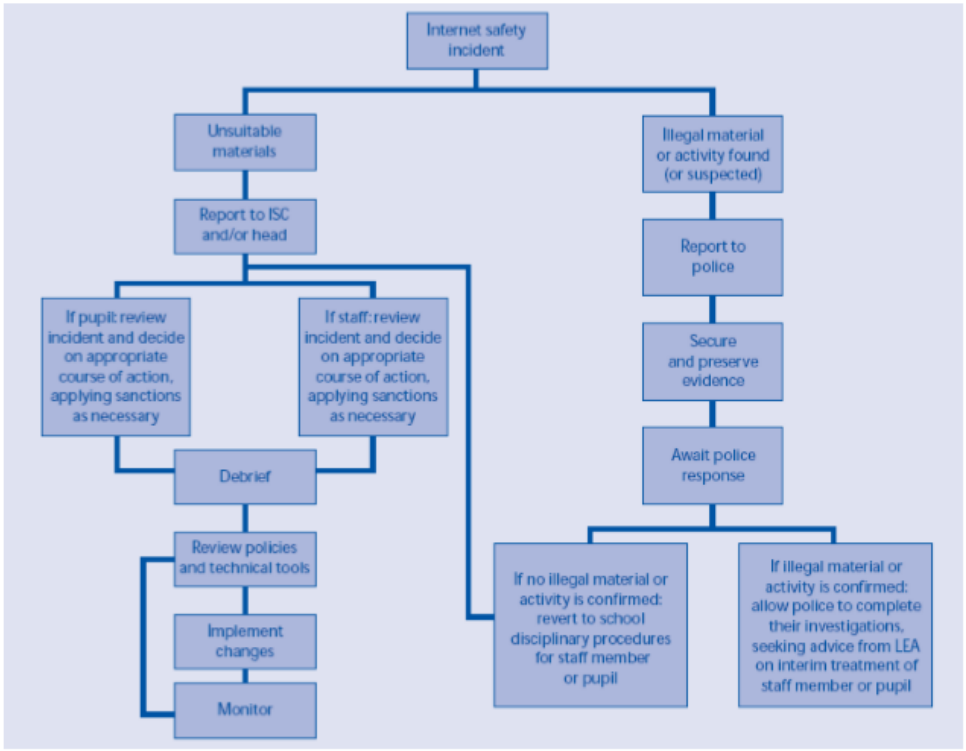
Incidents involving illegal materials or activities

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the Headteacher, then ultimately the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the Internet Safety Lead, network manager or Headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

E-safety and acceptable use

The following flow diagram shows the procedure for responding to incidents of misuse:

From E-safety Developing whole-school policies to support effective practice, Becta



From E-safety Developing whole-school policies to support effective practice, Becta

11. Sanctions

If a pupil misuses e-mail or the Internet, they must be reminded that this is irresponsible and contrary to their agreement with the Internet Acceptable Use Policy. They must agree to responsibly use the Internet and a further copy of the Acceptable Use Policy will be sent home for the child and parent to sign. A record of misuse will be logged by the Internet security co-ordinator. The child will not be allowed to resume the use of the Internet until the AUP has been resigned by the parent and child. Minor transgressions can be dealt with by the teacher as part of normal school discipline policy.

In serious circumstances the privileges of Internet use will be withdrawn for a fixed period of time.

12. Monitoring

The Internet Safety Lead will monitor any logged incidents and assess their importance.

Pupils will be informed there Internet use can be monitored. Monitoring checks will be made if any inappropriate use is suspected.

The Internet Safety Lead will report on incidents and the effectiveness of the e-safety policy to the governing body on an annual basis.

Review Due to the nature of the Internet and developing technologies this policy will be reviewed regularly as and when directed by the Health & Safety Policy Group or as part of a bi-annual review.

E-safety and acceptable use

References and resources

Keeping Children Safe in Education 2019

'E-safety - Developing whole-school policies to support effective practice',. Becta

Signposts to Safety – Teaching e-safety at KS1 and 2', Becta

Kent National Grid for Learning – Schools Internet Policy 5th Edition

www.becta.org.uk

www.pin-parents.com

www.nchafc.org.uk/Internet/index.html

www.vodaphone.com/content/parents.html

www.childnet.com/parents-and-carers

www.saferinternet.org.uk/advice-and-resources/parents-and-carers
www.thinkuknow.co.uk/parents