E-Safety Policy

Agreed by governing body – 17/3/2020

Ackworth Howard Church of England (VC) Junior and Infant School

Educating for 'life in all its fullness.'

Providing opportunities for growth in mind, body and spirit through inspirational and innovative education underpinned by a deeply Christian ethos. Those who learn and work here will develop confidence, embrace creativity and enhance their knowledge and skills so that they can experience 'life in all its fullness.' (John 10:10)

Values Statement

The Howard School is proud of its Christian ethos and values. Our pupils are proud to be responsible, thoughtful and motivated people who strive to do their best. As a Church of England school, the leadership, its teaching and the experiences it offers, will be underpinned and rooted in our Christian values, and in particular friendship, compassion, forgiveness and trust.

School E-Safety Policy context

The wider use of emerging technologies is important in order to enhance teaching and learning in schools. Access to the internet using a wide range of devices is 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 e-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 e-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 i.e. web-based resources, the use of Learning Platforms, email and other web based technologies such as blogs. Access to life-long 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 e-safeguarding. 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.

Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the children visit. Processes are in place for dealing with any unsuitable material that is found in internet searches.

- Requests for unblocking a website can be made through our technical support partners MINT, these requests should be auditable, with clear reasons for the need.
- 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. Real world examples of ‘Fake News’ are used and can be seen on the Computing display, for example.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. For example, children are taught to select ‘Creative Commons’ images when using them in their work.

Education

Pupils

Online safety education will be provided in the following ways:

- An online safety programme will be provided as part of the Computing curriculum as well as E-Safety day.

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 programme of assemblies, parental meetings 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.
- 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 when appropriate. They will be supported in delivering the message of online safety at home and our Safer Schools Officer will support in this area through parent information session and individual support at school or parent request.

Parents should inform school of any incidents outside of school that we need to be aware of, so we can take appropriate action – e.g. a child being bullied on X Box Live. This is important as it would lead to class teachers delivering sessions related to online conduct and repercussions etc.

Training and Staff

A programme of 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 schools e-safety policy and Acceptable Use Policies.
- E-safety policy and its updates will be presented to and discussed by staff / governors / governor meetings / INSET days etc.
- The e-safety Coordinator will provide advice / guidance / training as required to individuals as required.

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

Filtering and Monitoring Inappropriate Activity

RM filtering is used to block sites not relevant to educational use. A user account has been set up to access a platform (RM Safety Net) that can produce reports of inappropriate computer use. Any flagged use will be emailed directly to the Headteacher and appropriate action taken. Action will include use of the Behaviour Policy and reactive measures such as the use of the Be Internet Legends scheme of work produced by Google and Parent Zone.

Extended Schools

At Ackworth Howard School we offer a variety of opportunities when appropriate.

- Parental courses / meetings in computing, media literacy and online safety so that parents and children can together gain a better understanding of these issues.
- Messages to the public around online safety are also targeted towards grandparents and other relatives as well as parents through the school website, letters, leaflets and other relevant publications.

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 MINT (technical support). It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safeguarding responsibilities:

- School computing systems will be managed in ways that ensure that the school meets any e-safeguarding technical requirements and Acceptable Usage Policy and any relevant Local Authority e-safety policy and guidance.
- There will be regular reviews and audits of the 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, MINT.
- Requests from staff for sites to be removed or added from the filtered feed will be considered by the Headteacher.
- Appropriate and relevant security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices
- 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 web site / Facebook page

Staff or pupil personal contact information will not 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. Group photographs rather than full-face photos of individual children will be generally used.

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

Pupil image / 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 with the exception of the school's Facebook page. Staff are aware that if they choose to access social networking sites during their own time no reference should be made about Ackworth Howard 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
Complaints of technological misuse will be dealt with by a senior member of staff. 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.