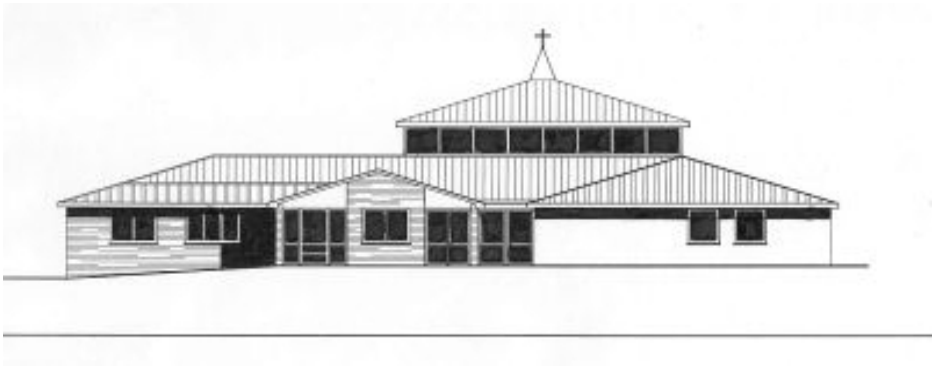

Holly Hill Methodist Church of England (Aided) Infant and Nursery School

Our Vision

Holly Hill embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. **In The context of Christian Care and Commitment *Holly Hill*** aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises. eSafety is not limited to school premises, school equipment or the school day. eSafety is a partnership concern that involves all at all times.

Holly Hill eSafety Policy

Parents and staff need to understand the different uses of technology both at home and in school. Following the New Curriculum in 2014 Safety now will be covered as part of the Curriculum and have its own scheme of work. Also the new Computing Curriculum will also support the new computing POS's for eSafety.

Related Documents:

Acceptable Use Policy for Adults

Acceptable Use Policy for Young People

Data Security Policy

Behaviour Policy

Anti-bullying Policy

Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/eSafety)

AUP's in context: Establishing safe and responsible behaviours

CAS – The New Computing Curriculum

Switched on to Computing

South West Grid for Learning

Hertfordshire County Council

Implementation Date: September 2014

Reviewed and updated: July 2016

Holly Hill eSafety Policy

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this:

- This Policy is available at our school website -
- This Policy will be updated every year .This will be done at the beginning of the academic year or sooner if current policy is changed or updated.
- E-Safety information is available at all computer points in school. A copy of the AUP is also there.
- Parents will be updated with current information on parents days .It is also available on request at the school office.
- The eSafety scheme of work will be available on request.

Currently the internet technologies children are using both outside and inside the classroom include – websites, VLE's, tablets with web functionality, emails, blogs, podcasts, video and music downloading.

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to *Mr Mark Carr* and our designated senior person for child protection. They are the central point of contact for all e-Safety issues and will be responsible for day to day management. The school has established an e-Safety committee that are responsible for policy review, risk assessment, and e-safety in the curriculum. The current members are:

Miss Charlotte - Taylor Head Teacher

Current DSP

Mr Mark Carr - eSafety Officer

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

All Staff in the School will sign the AUP annually and report incidents to above named staff who will help them complete an incident form should it arise.

Here is a clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml

Physical Environment / Security

Holly Hill endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the e-Safety log for audit purposes.
- Requests for changes to the filtering will be directed to the e-Safety co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the e-Safety log for audit purposes

- The school uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
- Only school devices may be attached to school computers. USB sticks are available on request.

Pupils use is monitored by *Mrs J Ingleby and the Headteacher.*

Staff use is monitored by *Mrs J Ingleby and the Headteacher*

- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office
- Key stage one pupils have their own login and document folders to keep their work in. Children also have individual login to RMeasimaths, purple mash, moodle and have individual emails.

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop/mobile device for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Pictures / videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'. The school e-mail system is provided, filtered and monitored by Link2ICT and is governed by Birmingham City Council E-mail Use Policy

- All staff are given a school e-mail address and understand that this must be used for all professional communication.
- Please do not open any unknown/suspect emails – report to eSafety Officer.

- Key stage one pupils have access to class based e-mail accounts that are monitored by the class teacher
- All pupils can be given their own school email accounts when considered necessary to assist them with research and when the need for a greater audience is required. They will be shown how to use it safely.
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staffs are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible and report procedure followed
- All Governors are given access to school network and understand that this must be used for all professional communication and have signed the current AUP.
- Emails created or received as part of your school job will be subject to disclosure I response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
    - Delete all emails of short-term value
    - Organise email into folders and carry out frequent house-keeping on all folders and archives
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive email
- Staff must inform (the eSafety co-ordinator or line manager) if they receive an offensive email
- Activate your 'out-of-office' notification when away for extended periods
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments
- ICT authorised staff may, without prior notice, access the email account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

Published content

The Head takes responsibility for content published to the school web site but delegate's general editorial responsibility to *Mr Mark Carr and Mrs J Ingleby* Class teachers and Key Stage co-ordinators are responsible for the editorial control of work published by their pupils.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office
- The school does not publish any contact details for the pupils
- The school encourages appropriate, educational use of the school web site and The Virtual Learning Environment - Moodle.
- Children and parents will be given guidance on their usage. Anything found to be unacceptable will be referred to the Headteacher.

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in line with Becta guidance and not identify any individual pupil
- Students' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Supervision of video conferencing will be appropriate to the age of the pupils

Publishing work on the website

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/transmitted on a video or webcam
- On the schools learning platform or Virtual Learning Environment
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, ie exhibition promoting the school
- General media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg, divorce of parents, custody issues etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Social Networking and online communication

Holly Hill is an Infant and Nursery School and therefore use of Social Networking site for pupils, is not applicable. However, Staff need to be aware of it and use it responsibly.

For adult use guidance is provided to the school community on how to use these sites safely and appropriately. This includes

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content
- cyber bullying

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites.

Parents wishing to use this facility on our website will receive guidance on acceptable and unacceptable use.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Google images and you tube may not be used to search whilst children are present
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
- The introduction of Moodle into the school allows Teachers to give access to relevant web sites that the students can use safely in a protected area. All students have their own user name and passwords. Access is restricted to their own Class area and the Parents Area.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity – children must not be allowed to change programmes unless under the direction of the Teacher/adult present
- Children must never be left unattended with either computer or tablet
- Staff and students will be expected to reference all third party resources that are used and be respectful of copyright
- All school data is encrypted when taken off school site

E-safety training

The school have completed a baseline assessment of current staff skills and have a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- There is an induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by

Mr Mark Carr ICT Co-Ordinator, e-Safety officer

and disseminated through staff meetings and training sessions

- E-Safety is embedded throughout the school curriculum and visited by each year group. This will be via the eSafety Scheme of work and through the current Computing Scheme of work for both Early Years and KS1
- Pupils are taught how to validate the accuracy of information found on the internet
- Parents sessions are available to provide appropriate advice and guidance
- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- A moodle course with eSafety resources is available to all teachers. This includes our new safety curriculum
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities etc.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998

Data is stored on the school systems and transferred in accordance with the Local Authority Data Security Guidelines

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office

Equal Opportunities

All adults and students using the school will be given access to the technologies available and appropriate support and equipment will be put into place to assist them

.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken inline with school anti-bullying and child protection policies. There may be occasions when the police must be involved.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate
- An incident log is kept in the school office. All incidents should be reported promptly.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We will be regularly consulting and discussing eSafety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg on school website)
- Parents will also be asked to give permission for their child to have a scratch account in school for school use
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
    - Information and celebration evenings
    - Practical training sessions
    - Posters
    - School website
    - Newsletter items