Church Hill Infants

E-Safety Policy

This policy was reviewed and adopted in January 2016

Reviewed March 2017

Reviewed October 2019

Signed(Chair)_____

Dated_____

Adopted January 2016
Reviewed March 2017
Reviewed October 2019

Adopted January 2016
Reviewed March 2017
Reviewed October 2019

Appendix G: Data Protection Policy
Appendix H: Management and information system
Appendix H: Support services
Appendix I: List of authorised persons

Church Hill Infant School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at *Church Hill Infant School* want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

The nominated senior person for the implementation of the School's e-Safety policy is the Headteacher.

Creating a Safe ICT Infrastructure in School

All users of the school's computer network have clearly defined access rights, enforced using a username/password login system. Account privileges are achieved through the file/folder permissions (through office 365), and are based upon each user's particular requirements – children have much more limitations in place through a standard year group login than individual staff members do with their personal logins, for example. This helps to protect the network from accidental or malicious attempts to threaten the security of it or the data accessible using it.
A permanently-enabled filtering system is provided, which is designed to filter out material found to be inappropriate for use in the education environment. As an additional safety measure, each individual web page is also dynamically scanned for inappropriate content as it is requested, categorised by its content and then access prevented to it if necessary.

Access to make changes to over-right the base-default setting to allow or deny access to a particular website URL can be achieved by contacting the ICT co-ordinator. All changes made to Internet filtering are logged by them to help prevent abuse of the system.

Security software is installed on all *Windows* machines to prevent any malware (e.g. virus) attacks. Staff laptops, are encrypted with a secure password.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential to halt impersonation on the network.

Rules for Publishing Material Online (inc. Images of Pupils)

Whilst we wish the school's website *and Twitter account* to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website *or on Twitter, (see app 1)*, the following principles should be borne in mind, in accordance with the school's *Safeguarding Policy*:

- If an image/audio/video recording of a child is used then they should not be named (including in credits).
- If a pupil is named, their image/audio/video recording should not be used (no surnames should be published).
- Files should be appropriately named in accordance with these principles and care should be taken to include only suitable ALT tags as well.
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website or *School's Twitter page.*
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published.

Comments submitted to posts on the website *or School's Twitter page* must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).

Children will likely use a variety of online tools for educational purposes during their time at the school. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photo/videos of school events (e.g. plays) are permitted to be taken by watching parents for personal memories, they will be asked not published them onto any public area of the Internet, including social networking sites.

It is important to remember that there can be very sound and in some cases reasons concerning child protection of why parents/ carers would not want some images published.

If there is no consent from the parent, then no filming of photographs will be taken that could identify the individual child.

Photography or Filming by parents

It is natural for parents to want to capture memories of their child at school during special events (nativity, concerts, sports). However, issues can arise when photography/video recording/ filming takes place at such events. These could include:

- Disturbance to other members of the audience
- Distraction to those pupils taking part
- Copyright restrictions
- Parental objection
- Child protection concerns

The decision on whether or not to allow photography, filming or video recordings rests with the Headteacher in consultation with the Governing Body. The decision would have to be taken in light of individual circumstances and the issues raised above, together with the circumstance surrounding the school such as size of hall, number and age of children participating. Any decision will be communicated to parents in writing well in advance of any performance. Where an objection has been raised by a parent to not allow their child to be included in any such photographs the school will consider ways in which to overcome these difficulties.

Where photography or recording of an event or performance is not allowed, the school will consider alternatives such as:

- Professional group photography arranged by the school.
- Individual photographs arranged by the school.
- Allowing parents opportunity to photograph before or after the event itself, where the objector would be able to withdraw their child without affecting the actual event or performance.

Only images of pupils in suitable dress will be taken to reduce the risk of images being used inappropriately. Particular care should be taken during PE, sports lessons.

Pupils' Rules for Acceptable Internet Use

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes.

- I will ask permission from a member of staff before using the Internet.
- I will respect the facilities on offer by using them safely and appropriately.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect other pupils and myself.
- I will be polite and respect others when communicating over the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details for websites with others.

Adopted January 2016
Reviewed March 2017
Reviewed October 2019

Staff/Governor's Rules for Acceptable Internet Use

Staff and governors are contractually obliged to use the Internet safely, appropriately and professionally within school. They are aware that they are role models for others and so should promote and model the high expected standards of behaviour at all times.

Whilst checking of personal sites (e.g. emails) is permitted outside of pupil contact time, it is recognised that this should only happen for brief periods of time and is merely a privilege (not a right) and thus can be removed at any time.

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

Staff/Governor's Rules for Personal Mobile Use

This guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice and to protect against potential misuse. In the interests of equality, and to further promote safety, the guidance applies to any individual who has a mobile phone on site, including children, parents and visitors, as detailed below:

- Staff are not permitted to have their mobile phones about their person; lockers are available in the staffroom for secure storage. There is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks within the staff room.
- Visitors are risked assessed and may be requested to sign in their phones if working directly in school/ with children (e.g. Ed Psychologist/ Speech and language therapist).
- Other than in agreed exceptional circumstances, phones must be switched off and calls and texts must not be taken or made during lesson time or any time when supervising children or talking with parents.
- Staff are not permitted, in any circumstance to use their personal phones for taking, recording or sharing images.

Adopted January 2016
Reviewed March 2017
Reviewed October 2019

- Staff are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting.
- Parents, visitors and contractors are respectfully requested not to use their mobile phones in school. Should phone calls and/or texts need to be taken or made this should be done outside the school building to avoid unnecessary disturbance or disruption to others.
- Notices throughout school will be on display to ensure the expectation on the use of phones is adhered to by all.

Adopted January 2016
Reviewed March 2017
Reviewed October 2019

E-Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential e-safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

E-Safety education will be provided in the following ways:

E-Safety within the Curriculum

Early Years Foundation Stage and Key Stage 1
At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. Staff will use the Hectors World/Smartie *the* Penguin scheme of work to teach children about E-Safety. Once a year, the whole school will take part in an E-Safety day. This will include activities and lessons to educate children on how to be safe when using the internet.

E-Safety Training for Staff and Governors

Staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues. A log of this training is kept within school.

E-Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive e-safety education and information (e.g. via the school website) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety behaviour – this includes delivery via newsletters and the school website.

Guidance on the use of Social Networking and messaging systems

The school recognises that many staff will actively use *Facebook*, *Twitter* and other such: social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are

encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

In accordance with school's staff code of conduct, it is never acceptable to accept a friendship request from a child from the school, as in all cases children of infant age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors to again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.

Data Protection

All data held on the school's network is subject to the *Data Protection Act 1998* and the school's Safeguarding Policy.

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data is taken home on a school laptop or other portable storage media, it must be recognised that this data comes under the *Data Protection Act* and is subject to the school's Safeguarding Policy. Care must therefore be taken to ensure its integrity and security. It should be removed from any portable device including USB pens and memory cards as soon as possible. Staff are required to provide written consent to a responsible use contract before being allowed to take home school equipment (e.g. teacher laptops).

Where authorisation has been given to a specific user to use a potable storage medium (e.g. memory stick) it is his/her responsibility to ensure that it does not transmit any viruses onto the school's network. It is recommended that pupils refrain from using such media unattended.

Staff are encouraged to use the school's cloud/onedrive as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through login by a member of school staff. When accessing files on the cloud outside of school, multifactor authentication will be required.

The servers containing these networked drives are locked away each night as an extra security measure to prevent against theft.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

Responding to Unacceptable Internet Use by Pupils

Pupils should be made aware that all e-safety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however staff are trained in how to proceed following a breach of the *Rules for Acceptable Internet Use*, in accordance with the school's *Safeguarding Policy*. This includes guidance on preservation of evidence and immediate reporting – the school's child protection officer has overall responsibility for Internet safety so any misuse should be reported to them without delay.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet and email being withdrawn.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Responding to Unacceptable Internet Use by Staff and Visitors

Failure to comply with the *Rules for Responsible Internet Use* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, *Child Protection Policy* and the law. Misuse should be reported without delay.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to *The Headteacher* so this can be taken into account for monitoring purposes.

Policy Review

This policy is reviewed regularly to respond to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Adopted January 2016

Reviewed March 2017

Reviewed October 2019

Please read in conjunction with following policies
Acceptable Use
Safeguarding
Whistle Blowing
Social Media
EYFS Policy

Appendix 1

Church Hill Infant School, Twitter Account

@CHISThurmaston

Twitter is a great and instant way of sharing what's happening in school with parents. It can be used to re-inforce learning by showing parents what we have been doing in class, or sharing homework, attendance cup, school council, hall of fame, star readers etc.

However it is a social media site so please keep in mind the schools **Social media policy** and **acceptable use policy**.

Please see Michelle for log in details

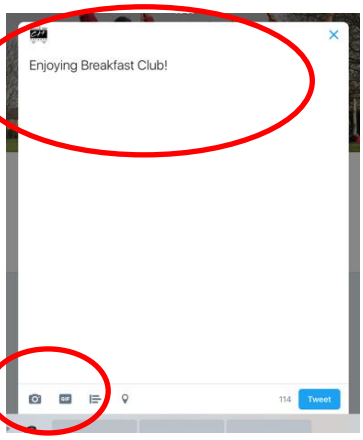
To help us all, here are a few simple **Ground Rules:**

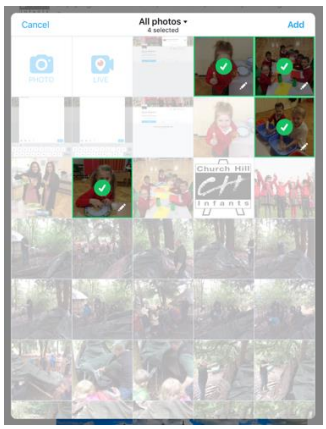
- Only post photos of children who have media & photo permission.
- Do not put any names of children. Only use (e.g.) class L/E or Year 2
- Photos work best when you add one or 4 pictures within a tweet.
- The account is a **one way communication tool.** This means:
    - Do not respond to messages or likes (if you do these will then show on our feed)
    - Do not follow anyone with the school account. (SLT are trialling this with a few accounts and this will be reviewed)
    - If you follow school with your personal account please be aware that parents will then be able to find you.
- If you use a # then the photos are more easily shared within the Twitter community.
- Please only use twitter on your school iPad. Remember you should not have photos of school children on personal phones.
- Remember once your tweet is out on social media it is potentially there forever. Please remember to check grammar, spelling and appropriateness of your tweet.
- Finally, if you are not sure – Don't Tweet.

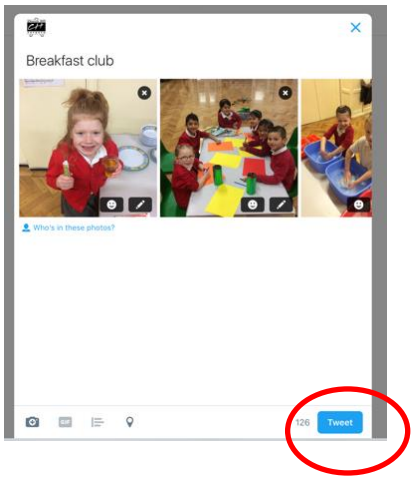
Adopted January 2016
Reviewed March 2017
Reviewed October 2019

How to Tweet

- Take picture(s) on your Ipad.
- Open your twitter app
- Make sure you are logged into the @CHISThurmaston account.
- Click on the feather/Quill (top right) and start your tweet.
    - Remember to keep messages short (140 characters max)
- Add photos by clicking the camera button and selecting your pictures.
    - 4 photos max. Then click Add
- Click on Tweet button & you are done.







Adopted January 2016
Reviewed March 2017
Reviewed October 2019