Kilham Church of England (V.C) Primary School
Millside, Kilham, Driffield, East Riding of Yorkshire, YO25 4SR
Tel/Fax: 01262 420214
Email: kilham.primary@eastriding.gov.uk
www.kilhamschool.co.uk
Headteacher: Mr R Palmer

Policy Front Sheet

Policy: E-Safety

Adopted: October 2019

Review Date: October 2021

Kilham CE VC Primary School e-Safety Policy

Introduction:

This policy is designed to describe how Kilham School; runs a safe, secure, internal network; allows safe access to the internet; controls data including information and photographs; responds to e-safety teaching requirements, cyberbullying and complaints.

The School Network

Security issues include:

- Access to all ICT systems (i.e school computers and internet use) shall be via individual and class logins and passwords. Members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the person in charge of data security. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where 'restricted' information is stored, access shall only be granted to individuals approved by the person in charge of data security.
- All access controls should be reviewed when users leave to ensure that any users have their access removed.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use, for example, secure storage of pupil performance data.
- Sensitive pupil data is stored on a separate network - 'admin pc'.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and must be password protected.
- Portable media may not be used without specific permission followed by a virus check – the only portable media sanctioned for use are school-issued encrypted USB drives.
- Unapproved software will not be allowed in pupils'/staff work areas or attached to email.
- Files held on the organisation's network will be regularly checked.
- The person in charge of network management will review system capacity regularly.

The Internet

Why is Internet use important at Kilham School?

- Internet use is part of the statutory curriculum and a necessary tool for learning – through the 2014 'Computing' element of the National Curriculum and as a cross-curricular tool.
- The purpose of Internet use in school is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance the school's management functions.
- However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

How will Internet access be authorised?

- In our primary school, all pupil usage of the internet should be fully supervised – a class login is used to gain network and internet access. Children sign an AUP, which is linked to our e-safety SMART rules.
- Parental permission is required for Internet access – this is given on entry to school.
- All staff must read and sign the organisation's policies regarding information security and the use of information technology before using ICT resources. This takes the form of a staff AUP – these are updated annually.

How will filtering be managed?

Levels of Internet access and supervision will vary according to the child or young person's age and experience.

- The school will use the LA mediated filtering systems to ensure that systems to protect children and young people are reviewed and improved.
- Requests for filtering changes from within the organisation will be made via the headteacher.
- Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children's Social Care, IWF or CEOP – this should be reported directly to the headteacher/Child Protection Coordinator.

How will social networking and personal publishing be managed?

Kilham CE Primary will control access to social media and social networking sites through ERYC filtering. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

However;

- Children and young people will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Children will be taught, through our e-safety curriculum, the dangers of placing personal photos on any social network space. They should consider how public the information is and the potential consequences.
- Children and young people should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children and young people should be encouraged to invite known friends only and deny access to others by making profiles private.

How can emerging technologies be managed and behaviour moderated?

- The new National Curriculum outlines statutory content in the computing curriculum which involves exploring new, collaborative ways of working using new technology.
- A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established.
- For example, if a class created a class blog or 'twitter' account, a brief risk assessment would be carried out prior to the work taking place. The safety and effectiveness of virtual learning and communities depends on users being trusted and identifiable – in cases where comments

or communications from unidentifiable sources is possible, safeguards will be put in place to moderate such communication before the children are exposed to it.

- Abusive messages or any kind of cyber-bullying will be dealt with under the organisation's behaviour and/or anti-bullying policies.
- Any technologies that use messaging services or online communication will not be used until parental permission is granted.

How will email be managed?

The implications of email use for Kilham CE Primary by children need to be thought through and appropriate safety measures put in place.

Un-regulated email can provide routes to children that bypass the traditional school boundaries and security measures.

At present, all email/messaging used by children is under the umbrella of 'Planet Sherston'. This system is completely internal, although can be accessed from home. Children do not have access to 'real' email from school. A 'virtual' email software application may be used to teach children email protocols.

Whole-class/group/project email addresses will be used in school for communication outside of the school – only if monitored by the class teacher.

- Children must not access webmail email accounts using school equipment.
- Children and young people must immediately tell an adult if they receive offensive email.
- Children are taught not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

The Control of Information and Data

How will published content be managed?

Websites can inspire children and young people to publish work of a high standard. Websites can celebrate children and young people's work, promote the school and publish resources for projects.

Sensitive information about Kilham CE Primary School and children will not be published in newsletters or on the school website.

Publication of information should be considered from a personal and school security viewpoint. (For example, names and images not used together)

- The contact details on the school website should be the school address, email and telephone number. Employee/volunteer or children and young people's personal information (apart from staff names and children's first names) must not be published.
- The headteacher monitors school website content and ensures that content is accurate and appropriate.
- The website should comply with guidelines for publications including respect for intellectual property rights and copyright.

How are pupil/work/events images used, stored and published?

1. Only school cameras should be used for any school-related photography.
2. Images taken must not be stored on teacher's laptops – images should be uploaded from the camera onto the school network.
3. In the EYFS, 2Simple '2buildaprofile' should be used for as many EYFS photo observations as possible – these images are stored securely on 2simple's servers before being used. All other images taken in EYFS need storing on school's server.
4. Children's names should not be used for file names.
5. With parental permission, newspapers occasionally use images of our children along with their names (Christmas play pictures/new starters etc.) Permission to use images is requested and updated upon entry to school.
6. On the school website, however, the publishing of children and young people's names with their images is not acceptable.

How do we manage mobile phones?

At Kilham CE VC Primary School we do not have a separate Mobile Phone Policy. The use of personal mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of the Headteacher and recorded. Personal mobile phones should not be used to take photographs or videos of children and/or school events – school cameras are available.

How will information systems security be maintained?

Data security is dealt with through other school policies - data protection, freedom of information etc. The person in charge of data security is the Headteacher. Note the role is distinct and separate from the 'E-safety co-ordinator'.

All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation.

E-safety Teaching Requirements, Cyberbullying and Complaints

How will children and young people learn safe practices?

A termly e-safety scheme of work is provided for all class teachers – this includes a range of resources but is based upon the 'SMART' rules. Our ongoing e-safety curriculum ensures that children are taught the reasons for caution in publishing personal information and images online. (see appendix)

How will complaints be handled?

- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (Teaching Online Safety in Schools) June 2019

- Cyberbullying (along with all forms of bullying) will not be tolerated in Kilham CE Primary School. Full details are set out in the school's policy on anti-bullying.
- All e–safety and cyberbullying complaints and incidents will be recorded by school - including any actions taken.
- All school policies, including complaints procedure, Child Protection, Safeguarding, Whistleblowing, Behaviour, Anti-bullying etc. apply to e-safety related incidents.
- Response to risk flowchart and E-incident Log pro-forma are attached to this policy.

How will risks be assessed?

- Kilham CE Primary will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither Kilham CE Primary nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.
- Kilham CE Primary will continually audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate, this includes identifying, assessing and minimising risk.
- On adoption of this policy, the e-safety coordinator and headteacher will complete a risk assessment for current resources, usage and ICT levels of risk.

Kilham CE VC Primary School - Acceptable Use Policy

ICT Equipment and Internet Rules

Before using school ICT equipment and using the internet in school, it is important that everybody understands some basic rules which will help us all stay safe online. These rules should remind you of the 'SMART' rules and the work that you do in E-Safety lessons.

I agree to keep my personal information safe
Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings.
Do not give out personal information like email addresses, home or school addresses or mobile phone numbers.
Only post photographs which you would be happy with your parents or carers seeing and make sure they do not show addresses. Do not share your passwords.

I agree not to access websites that are not suitable for my age and I will tell adults about anything I find that I am worried about.
I know how to use 'Hector' to cover up my computer screen.

I agree not to contact people I do not know using the internet or other technology (unless this is supervised and part of a lesson).

I agree to report any worries I have to an adult.
If anyone online makes you worried or says things that make you feel uncomfortable tell an adult.
Do not respond to upsetting messages and cyber-bullying. Keep the message and show it to an adult you trust.

I agree not to send unsuitable pictures or films to anyone using the internet.
By sending images of this type you could be committing an offence.

I agree not to use digital technology to bully people or make threats.
This is Cyberbullying and (like any other Bullying) is never acceptable. This includes using Planet Sherston properly and being kind when using friends and messaging.

I agree to follow the ICT Suite Rules:

1. I will only save and retrieve from my own documents folder.
2. I will not look in other people's folders.
3. I will not attempt to delete, install or move files.
4. I will not download files from the internet without permission.
5. I will not register on any site which asks for a name or password.

I agree to follow the "SMART Rules" to keep myself safe online
I understand that internet use at Kilham CE Primary School is closely monitored and individual use can be tracked.

Signed..... (Signed by the child) Date.....

Kilham CE VC Primary School - Acceptable Use Policy for Staff –

This Acceptable Use Policy is part of our E-Safety policy, designed to help Kilham School run a safe, secure network, allow safe access to the internet, control data including information and photographs and respond to e-safety teaching requirements, cyberbullying and complaints.
For more information see E-Safety Policy and 'Safeguarding – Guidance for Safe Working Practices' in the staff handbook.
The E-Safety Coordinator is R Palmer

The School Network

I agree to:

- be responsible for selecting and securing usernames and passwords.
- be responsible for keeping pupil data secure – i.e not in folders/areas that can be accessed by others.
- log off after using ICT equipment.
- ask permission before installing any software onto the network or using any portable device.

The Internet

I agree to:

- be responsible for supervising pupils at all times when they are using the internet.
- only access suitable material; I am aware that accessing materials which are unlawful, obscene or abusive is not permitted. I agree to report unsuitable material to the E-Safety Coordinator.
- follow the guidance given in the 'Safeguarding - Guidance for Safe Working Practice' policy, provided in the staff handbook.
- keep within copyright laws; I will respect work and ownership rights of people, including abiding by copyright laws.
- the responsible use of social networks, both within and outside the workplace; The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.
- not use unsecure email to transfer sensitive data – Encrypted USB drives are provided for this.

The Control of Information and Data

I agree to:

- only use school cameras for any school-related photography.
- upload all images onto the secure network and not store them on personal devices or laptops.
- be aware of the sensitive nature of publishing school related information, including pupil names and images – I will refer to the guidance in the e-safety policy.
- not use my personal mobile phone to take photographs of a school-related nature or for personal communication with children.
- be aware of data protection policies and know of their location and my liability in law.

E-Safety, Cyberbullying and Complaints

I agree to:

- refer any e-safety or cyberbullying incidents to the E-Safety Coordinator or headteacher, who will follow the 'Response to Risk Flowchart' and log the incident accordingly.
- refer to the school policies for guidance on following the complaints procedure, Child Protection, Safeguarding, Whistleblowing, Behaviour, Anti-bullying and any others that may apply to e-safety related incidents.
- refer any new curriculum project which involved internet use to the E-Safety Coordinator/headteacher before beginning (i.e new blogs)

Name (print)……

Signed……

Organisation……

Date……