Kirkby on Bain Church of England Primary School

Learning together for life

Online Safety Policy

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents

Safeguarding is a serious matter; at Kirkby on Bain CE Primary School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as online safety or e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

Upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils when they start school with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the internet.

Curriculum

Online safety is embedded within the National Curriculum 2014:

“Pupils should be taught to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.” (National Curriculum 2014, Computing, KS1)

“Pupils should be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.” (National Curriculum 2014, Computing, KS2)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our school.

The Headteacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, Governing Body, parents.
- All online safety incidents are dealt with promptly and appropriately.

Online safety Officer

The headteacher is the designated online safety officer and will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for school and home use.
- Review this policy regularly.
- Advise the Governing Body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support (Ark ICT)
- Make himself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff (Ark ICT) are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any online safety technical solutions such as internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer / Headteacher.
- Passwords are applied correctly to all users regardless of age.
- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online safety incident is reported to the online safety officer / Headteacher (and an online safety incident report is made).

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings and workshops, school newsletters and information on the school website, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Kirkby on Bain CE Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The computing subject leader, online safety officer and IT Support (Ark ICT) are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords – all staff and pupils will be unable to access any device without a username and password. iPads, however, are not password protected.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated for new virus definitions. IT Support (Ark ICT) will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy. Parents may sign on behalf of their child or children.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not advised.

Photos and videos –All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Kirkby on Bain CE Primary School is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Kirkby on Bain CE Primary School and have been appropriately risk assessed:

- Blogging – used by staff and pupils in school.
- School Twitter account – managed by the headteacher

Should staff wish to use other social media for school purposes, permission must first be sought via the online safety officer / Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.

- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of the online safety officer/Headteacher. The online safety officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Kirkby on Bain CE Primary School will have an annual programme of training which is suitable to the audience.

Online safety for pupils is embedded into the curriculum; whenever technology is used in the school, staff will ensure that there are positive messages about safe use and risks as part of the pupils' learning.

As well as the programme of training the school will establish further training or lessons as necessary in response to any incidents.

Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher.

Approved: February 2016 Review: February 2017

Acceptable Use Policy – Staff

Note: All internet and email activity is subject to monitoring

You must read this policy in conjunction with online safety policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; promoting terrorism and extremism or any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with pupils on personal social networks.

Use of email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or pupil.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal use of school ICT – School ICT equipment should only be used for personal use when specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) and personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the online safety officer.

Viruses and other malware - any virus outbreaks are to be reported to Ark ICT as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Online safety – like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with pupils.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

Note: All internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share personal information online with anyone.

I will not – download anything from the internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Pupil) :

Date :