Headteacher: Mr Jonathan Hart
Fritwell C of E Primary School
East Street,
Fritwell,
Oxfordshire,
OX27 7PX.

Tel No: 01869 345283
Email: office.3065@fritwell.oxon.sch.uk

Fritwell Church of England Primary School
East Street,
Fritwell,
Oxfordshire,
OX27 7PX

Fritwell Church of England Primary School

E-Safety Policy

"Growing and learning together with God."

Children at Fritwell Church of England School are confident and inspired. They achieve personal success and show love and respect for all.

Introduction

This policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of school. To help enhance our creative approach to the curriculum, we give children access to a range of digital devices. This is why we believe it is important that both staff and children understand the risks involved and know how to avoid them.

Aims and Objectives

The aim of this policy is to protect everyone involved in the school from being a participant in, or the victim of, illegal, offensive or harmful activities associated with modern electronic media.

- This policy lays out the acceptable use of computers, tablets, cameras, mobile phones and other portable devices in a way that can be understood and adhered to by everyone involved in the school.
- To promote the aims of this policy each class in Key Stage 1 and 2 is taught E-Safety in the Autumn Term.

Teaching and Learning:

The teaching of E-Safety is referenced in both our Computing curriculum, as part of the Digital Literacy topic, and in our PSHE curriculum.

We also provide other opportunities to promote E-Safety within school. For example: through school assemblies, during Anti-Bullying week, Internet Safety Day and hosting visiting experts.

Children, from Year 1 upwards, must sign the **Pupil ICT Acceptable Use Agreement** every year, before they are allowed access to the school's digital devices. This document will be discussed and signed by the children in school, and an unsigned copy will be sent home to parents for information.

EYFS UNIT

Many of the issues raised in this policy are not applicable to very young children in nursery and reception. However, when using the internet, children are taught how to stay on one website.

Electronic Communication with the School

- Children do not have email addresses at Fritwell C of E Primary
- All staff and governors have email addresses which are used for communicating with matters regarding the school and/or their class.
- We distribute information to parents and carers via text message and email as well as paper copies as requested.
- We publish relevant information on our website and we keep this regularly updated. Additional information such as policy documents can be downloaded as PDFs.
- We communicate via our Fritwell C of E Facebook page.

Servers, Passwords and Data Security

The licensed software we use for administration (MIS), Integris, is approved by Oxfordshire County Council, and any personal data is stored securely using this. We also use an internet filtering system, provided by our ICT support company 'Turn It On', which blocks viruses and inappropriate material.

- Various websites and servers require passwords when logging on. Children are taught the importance of always keeping these strictly to themselves.
- There are two servers on the school premises, an Admin Server and a Curriculum Server.
- The office staff and Headteacher have access to the Admin Server.
- There are three drives on the Curriculum Server, each with increasing levels of restriction:
  1. A pupil drive, to which all children and staff have access;
  2. A teacher drive, to which only staff have access via their server logins;
  3. An administration drive, restricted to the administrators and Senior Leadership Team.
- All user accounts are synchronised to the server, and automatically backed up.
- ICT Support Team have the ability to access users' documents, change all users' passwords and their computer access levels.
- Data is handled securely, sensitively and appropriately, in line with the requirements of the Data Protection Act (1998). Our servers are backed up every evening at 21:00 to an external hard drive stored in the resources room.

Working online

Children are supervised at all times when working online. In the unlikely event that any inappropriate material slips past our filtering system, children are taught to report it immediately to a member of staff. The ICT Leader keeps an Incident Log of all such incidents and Designated Safeguarding Lead will be informed and the site blocked manually.

Photographs and Videos

We seek permission from parents for the use of photographs and videos of children on our website, Facebook page, in newsletters and other publications. These forms are signed when children start at our school. Parents who change their minds about permitting publishing privileges should inform the school in writing. All staff are aware of the list of children for whom we do not have such permission.

- At Fritwell Primary School we have no wish to prevent parents or carers taking photographs or films of the children in our care. We cannot, however, give permission for their publication. Therefore, it is essential that permission is obtained from the parents of all children appearing in images that are to be, for example, uploaded to the internet by the person wishing to upload.
- Photographs uploaded to the school website or Facebook page will never identify children by name.
- All photographs and videos of children will be taken using school cameras or school iPads. Devices belonging to staff may be used with prior permission from the Headteacher for the purpose of uploading photos to the website and Facebook page. Photos are then removed from these devices as soon as possible.
- Pictures taken and stored on a school camera or iPad will be downloaded on to a school server and removed from the camera as soon as possible.
- School memory cards must not be used in other cameras.

Mobile phones and other portable devices

- Staff at Fritwell Primary may bring in mobile phones and other portable devices for their own use but may only use them during breaks or non-contact time, unless the device is being used for teaching and learning purposes. E.g. music stored on a smart phone.
- If a member of staff has a family emergency they may either seek permission from the Headteacher to keep their mobile phone to hand or they may use the school's or their own phone to make calls from the school office.
- Children are not allowed their personal mobile phones or other portable devices at school. If any such device is brought into school it must be left with their class teacher in the morning and then handed to a parent at the end of the day where possible. If teachers are unable to speak to a parent or carer directly, they should telephone to inform the family that these devices are not allowed on school premises.
- iPads and laptop computers are used in school. The children are supervised at all times when using portable devices that can access the internet. These devices use the internet filtering system provided by Turn It On as referred to above.

Safeguarding

It is the responsibility of all members of staff to be vigilant and report any concerns they might have about pupils in school to the ICT Leader. Any concerns regarding staff should be reported to the Headteacher.

- Any incident where inappropriate material might have been inadvertently seen by a child at school must be reported to the class teacher and ICT Leader, who will log this. Appropriate action will then be taken (E.g. review filtering software). The Designated Safeguarding Lead and parents will be informed if deemed necessary.
- If inappropriate material is deliberately accessed by a pupil, this must be reported immediately to the DSL and safeguarding procedures must be followed. The incident must be logged, and a record kept in the safeguarding file.

- Any safeguarding concerns which relate to a member of staff should be reported to the Headteacher. If there is a concern about the Headteacher, then the Chair of Governors should be informed. Safeguarding / whistleblowing procedures should then be followed.
- We encourage children to discuss any anxieties they may have regarding inappropriate material they might have seen outside school, and to report instances of cyber-bullying outside of school.
- See Safeguarding Policy for further information.

Involving Parents

Children have increasing access to digital devices, which enables them to access the internet outside of school. The school sends out information regularly to parents about these dangers and how to handle them.

School Community

Regular visitors to the school are given a handbook, which contains this policy. It is also available on our website.

Roles and Responsibilities

- The ICT Leader will deal with any e-safety incidents in the first instance and record them in the Incident Log. These will then be escalated to the Headteacher if necessary.
- The ICT Leader is also responsible for monitoring the delivery of the agreed Computing Curriculum and logging any incidents.
- The Headteacher is responsible for ensuring the policy is implemented, that e-safety is included in Safeguarding training and that staff are full trained.
- Teachers in the school have a responsibility to deliver the agreed E-Safety units for each year group (to be taught during the autumn term) and support any additional events we are running within school e.g. Anti-Bullying week with an E-Safety focus.
- It is the responsibility of the Primary Leadership Team to help make the E-Safety Policy child friendly and communicate its message to other children in the school.
- The school Governors are responsible for its review.

Monitoring and Reviewing

The effectiveness of this policy will be continually considered by the ICT Leader, Senior Leadership Team and the Governors in light of any incidents of concern. It will be reviewed every two years, taking new technologies into account.

Date of Policy: March 2020
Review Date: March 2022