E-safety Policy

Our Vision
We are a family-orientated school where everyone is welcome, a place where we strive to provide the best possible education in a caring Christian environment; an education that allows everyone to flourish and have the confidence to make a positive contribution. We seek to develop the individual strengths of everyone within our school community, where each unique personality can be recognised and valued.

Our Christian values underpin everything we do: Thankfulness, Kindness, Forgiveness, Fairness, Friendship, Trust, Hope and Inclusion are key priorities for all pupils and adults in our school.

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

Users - refers to staff, governing body, school volunteers, students 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, volunteers, governing body, parents

Safeguarding is a serious matter; at Uffington Church of England Primary School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as 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.

This policy is available for anybody to read on the Uffington Church of England Primary School website. All members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy on an annual basis in preparation for the new academic year, or sooner should there be any significant changes to policy upon review.

Policy Governance (Roles & Responsibilities)

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 e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-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 e-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 e-safety within our school.

At Uffington Church of England Primary School, the Headteacher is also the e-Safety Officer. The Headteacher ensures that:

- E-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 e-safety incidents are dealt with promptly and appropriately.

In the role of e-Safety Officer, the Headteacher will:

- Keep up to date with the latest risks to children whilst using technology; familiarising him/herself with the latest research and available resources for school and home use.
- Review this policy regularly
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with ARK ICT Solutions and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with ARK ICT Solutions.
- Make him/herself aware of any reporting function with technical e-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

The school procures the service of ARK ICT Solutions to manage its network. ARK ICT Solutions 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 e-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 e-safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

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 e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Pupils

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

e-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 assist parents to gain the skills and knowledge they need to ensure the safety of children outside the school environment. Through information published on the school website and school newsletters, the school will endeavour to keep parents up to date with new and emerging e-safety risks.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the school's Single Consent Form before any access can be granted to school ICT equipment or services.

Technology

Uffington Church of England Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use NetSweeper software that prevents unauthorized 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.

Email Filtering – we use NetSweeper 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.

Encryption – All school devices that hold personal data (as defined by the General Data Protection Regulation 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such

as laptop or USB pen drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner'sOffice.
(Note: Encryption does not mean password protected.)

Passwords – all staff and students will be unable to access any networked device without a unique username and password. Pupil passwords will change if there has been a compromise. Staff are encouraged to change their passwords on a regular basis. ARK ICT Solutions will be responsible for the management of user names and passwords. Pupil iPads are not passcode protected.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ARK ICT Solutions 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 this e-safety and the staff Acceptable Use Policy; pupils upon their parents / carers signing and returning their acceptance of the Acceptable Use statement included in the Single Consent Form. The headteacher receives a weekly Securly Activity Report which provides information about the websites staff and pupils request to access which may be checked in the event of a concern about inappropriate browsing.

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 permitted.
Pupils are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of the following: firstname.secondname@uffingtonprimary.co.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Safe Use of Photographs Policy, and is re-iterated here for clarity. All parents must sign the Single Consent Form stating whether they wish images including their children to be used for marketing and publicity purposes 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; Uffington Church of England Primary School is fully supportive of social networking as a tool to engage with parents and the wider school community. Any new service will be risk assessed before use is permitted. At the present time, the school uses Facebook as a broadcast service which is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such, no two-way communication will take place. Those viewing Facebook posts may *'like'* or comment on the information. Comments are monitored closely to ensure that they are appropriate and fair; where this is not the case, further action will be taken to remove / prevent inappropriate comments.

Video Conferencing – The school uses Google Meet, Zoom and MS Teams for meetings and remote teaching. The Code of Conduct for Staff applies to video conferencing whether the host or participant is working at school or from home. Any meetings involving children are hosted by a member of staff; the host is responsible for safeguarding during any sessions. If a meeting involving children is hosted by someone from outside school, a member of staff is always present and it is the responsibility of that person to ensure that children are safe. Any concerns regarding the safety of children must be reported to the eSafety Officer / DSL immediately.
When hosting a meeting from home, staff must ensure that they are appropriately dressed and be mindful of what is in the background. If, during a live session, the host sees or hears something which raises a safeguarding concern, this must be reported to the eSafety Officer / DSL immediately. It is the host's responsibility to ensure that all communications, whether verbal or in 'chat' form are appropriate.

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

- The Single Consent Form must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students by name.
- 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 school's 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 e-safety incident is to be brought to the immediate attention of the Headteacher who will then assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

MultiFactor Authentication:

The school has adopted MFA / 2FA authentication to provide secure access to school data and email from non-school devices or out of school. This is designed to protect against phishing attacks, where user credentials are harvested.

Cyber Bullying

Cyber Bullying can be defined as the use of Information and Communication Technology (ICT), particularly mobile phones and the Internet, to deliberately upset someone. Uffington Church of England Primary School is committed to ensuring that its pupils are made aware of the issues surrounding cyber-bullying at a level appropriate to their age and stage of development. Should an incident of cyber-bullying affecting a pupil come to the attention of a member of staff, either within or outside school, the Headteacher should be informed immediately. Such incidents will be dealt with in line with the school's Anti-bullying Policy.

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, Uffington Church of England Primary School will have an annual programme of training which is suitable to the audience.

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

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

The Headteacher/ e-Safety Officer is responsible for planning a programme of training and awareness for the school. 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 for further CPD.

The e-Safety Training Programme is included in the Six-Year Safeguarding Training Pathway.

This policy has been agreed by the staff and Governing Body and is reviewed annually.

Policy reviewed by the Curriculum and Standards Committee	February 2024
Next review	February 2025