Christ Church CE (C) Primary
E-Safety Policy

The Internet is regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using Information, Communications Technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. The children also use the internet to access our school's Learning Platform through Microsoft Teams.

Computer skills are vital to access life-long learning and employment; Computing is now seen as an essential life-skill. ICT skills and resources are used daily to support and enhance the learning of the children at Christ Church.
Young people have access to the Internet from many places: home, school, libraries and in many cases mobile phones and tablets.

Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. This policy is designed to ensure safe internet use by pupils in school and give them the skills and awareness to remain safe while on-line at home.

The purpose of this policy is to:
- Set out the key principles expected of all members of the school community at Christ Church Primary School with respect to the use of ICT-based technologies, including the use of our Learning Platform.
- Safeguard and protect the children and staff of Christ Church Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Links to other policies and national guidance:
In conjunction to this policy, the following school policies and guidance should be referred to:

- Safeguarding Policy
- Whistleblowing Policy
- Behaviour Policy
- CCTV Policy
- Computing Policy
- Use of mobile phones in the foundation stage toolkit
- Staff code of conduct
- Remote Learning Policy
- Remote Learning Acceptable Use Policy

The following national guidance should be read in conjunction with this policy:
- PREVENT Strategy HM Government
- Keeping children safe in Education (DFE September 2020)
- Teaching online safety in schools (DFE June 2019)
- Working together to safeguard children

Our whole school approach to the safe use of ICT:
Creating a safe ICT learning environment includes three main elements at this school:
- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- Embedding E-Safety teaching into the school curriculum

Staff Training:
Staff at Christ Church C of E Primary School, receive regular information and training on E-Safety issues, as well as updates as and when new issues arise. All staff members are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety. Staff members are encouraged to incorporate E-Safety discussions and activities within various areas of the curriculum.

School Internet provision:
The school use a Staffordshire approved content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.
• All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
• Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

At the start of each academic year, an *Internet use agreement* is sent home with all children from Reception to Year 6. This letter highlights the use of ICT within the classroom and the importance of being responsible when using the Internet at school. Six Internet safety rules are set out in the letter to be discussed by parents/carers at home with their children. The letter is then signed and returned to school.

Home Internet provision:
Whilst school understands that they have no control over the internet content which children are exposed to when at home, we instead work hard to educate both parents/carers and the children about how to stay safe online. This is done in a variety of different ways:
- E-Safety lessons with the children
- E-Safety worships for the children
- E-Safety workshops for parents/carers
- E-safety updates in the fortnightly newsletter to parents/carers
- E-Safety newsletters every term
- Sharing the Remote Learning Acceptable Use Policy with parents/carers (Appendix 1)
- Discussions with parent/carers when incident arise

Downloading files and applications:
The internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.
Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

Portable storage media:
Staff and children are not permitted to use their own portable media storage (USB Sticks, External Hardrives etc) to school related data. To save resources onto the school system from home, staff log into the school e-portal.

Teaching and Learning:
We think it is crucial to teach pupils how to use the Internet safely, both at school and at home. We use a number of different services and websites to support this, including the Kidsmart safety code:

 - Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk
The main aspects of this approach include the following five SMART tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

E-Safety is frequently discussed in lessons, during class worships and in whole school worship so that children are kept up to date. There is an e-safety section of the newsletter every fortnight and there are yearly parent/carer workshops about E-Safety.

Why Internet use is important:
The Internet is an essential element in 21st century life for education, business and social interaction. As a school Christ Church has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The internet is also essential for children who are unable to attend school to access our Learning Platform. School works closely with the families in our community to ensure that they have internet access and devices to use for educational purposes when at home. (See our loaning devices agreement, appendix 2.)

Internet use enhances learning:
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Parents/carers and pupils are provided with a copy of the Remote Learning Acceptable Use Policy to ensure that behaviour online is acceptable.
- Internet access is planned to enrich and extend learning activities.
- Staff members guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils are taught how to evaluate Internet content:
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Deputy Head Teacher, Computing Lead and/or a Designated Safeguarding Leader.
- Staff members ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access:

1. **Information system security**
- The security of the school information systems are reviewed regularly.
- Virus protection is installed and updated regularly.
- The school uses broadband with its firewall and filters.

2. **E-mail**
- Staff members only use an approved individual school email account which is allocated to them by the school.
- Staff do not use personal email accounts for professional purposes, especially to exchange and school related information or documents or to email parents/carers.
- Year groups teachers have a specific email address for parental queries regarding the remote learning. Any other parental queries coming to these addresses will be forwarded onto the school contact@ address.
- Year group emails are frequently monitored by members of the Senior Leadership Team to ensure correct conduct is adhered to.
- Staff members do not email parents/carers directly from their individual school email accounts.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive an inappropriate or offensive email.

3. **Published content and the school website**
- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils personal information is not published.
- The Head Teacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

4. **Publishing pupil's images and work**
- Pupils' full names are not used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website.
- All parents / carers are asked for permission for their children's photograph to be taken and uploaded to the school website. At no point is a photograph uploaded online with a child's full name.

5. **Social networking and personal publishing**
- Social networking sites and newsgroups are blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents are advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- In November 2014, a school Twitter account was set up. The account is 'locked', ensuring that only people who the school approve are able to access our 'tweets'. As Twitter is not intended for use by any person under the age of 13 years old, we do not accept pupils as followers. Our 'tweets' are not public or searchable and are only viewable by those who we approve as followers. Only those children who the school have permission for are photographed for Twitter and no child is named on the social media site.
- Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold social networking accounts should not have parents or pupils as 'friends'.

6. **Mobile phones**
- The use of mobile phones is not permitted within school by children
- The use of personal mobile phones is not permitted across school.
- There are two school mobile phones which are used to capture photos and videos of the children taking part in events both inside and outside of school. These are clearly labelled and are stored in the HT's and DHT's offices.
- Those children who choose to bring a mobile phone to school hand them in to their class teacher where they are kept in a secure place until the end of the school day.

Managing filtering:
As a school we work closely with Entrust and have Policy Central Enterprise (PCE) installed on all school devices. PCE detects potentially inappropriate content and conduct as soon as it appears on screen, is typed in by the user or is received by the user. A screen capture is taken of every incident detailing the time and date of capture. The school works in partnership with the service provider to ensure filtering systems are as effective as possible. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety leader.

Protecting personal data: *(Please see the school Data Protection Policy)*
Personal data will be recorded, processed, transferred and made available in accordance to GDPR.

Appendix 1:

Christ Church CE (C) Primary School
Microsoft Teams: Remote Learning Acceptable Use Policy

Parental Acceptable Use Policy:

I understand that:

➢ Teams activity is monitored by staff and any inappropriate content or concerning or disruptive behaviour is reported to ensure all students are following the expectations for accessing Teams;

➢ Students who do not adhere to the expectations below may be removed from any online live lesson or activity and will be referred to a senior leader, Deputy Head Teacher or Head Teacher as appropriate;

➢ Parents will be contacted if their child is not adhering to the expectations set out below.

Pupil Acceptable Use Policy:

In addition to any Acceptable Use Policy at the school, I understand that when using Microsoft Teams:

➢ There is an expectation that I will engage in online collaborative work when requested by my teacher.

➢ I will work in a respectful and helpful manner, following instructions carefully.

➢ The recording of still images, filmed images or audio of teacher/teaching assistants or other pupils without permission, and the distribution of such images, is **strictly forbidden**.

➢ The use of pre-recorded videos for other purposes such as TikTok videos is strictly forbidden as above.

➢ Making inappropriate, offensive or unkind comments, including through emojis and/or images, is not be tolerated.

➢ The chat function **is not** used at our school.

➢ I will be polite and friendly in all interactions online.

➢ I will not interfere with another student's work without their permission whether it is work submitted on a platform or shared work in a collaboration space.

➢ When submitting work, I must adhere to the usual standards of honesty and be careful not to plagiarise work, avoiding copying off the internet and submitting as my own work, or submitting work as my own without reference to others if the work was generated collaboratively.

I understand that when using Microsoft Teams for online live lessons:

➢ My teacher will start and end all online live lessons. I **will not** set up my own meetings.

➢ My teacher will be in control of the webcam and discussion function at all times:

- o there will be times when microphones should be muted and times when they should be on;
- o there will be times when cameras should be on and times when my teachers may ask me to turn my camera off.

➢ Live online lessons will be monitored closely at all times but will not be recorded due to GDPR.

➢ Behaviour when working as part of any online live lesson should be the same as when we are at school. We show:

- o respect for other students and staff;
- o that we are listening;
- o prepared to ask and answer questions;
- o attempt the learning activities to the best standard that we can;
- o talk and act respectfully and enthusiastically with others.

<u>**Appendix 2:**</u>

IPad/Laptop Loan Agreement

This agreement is between:

1) Christ Church CE (C) Primary School, Lichfield ("the school")

2)   ("the parent/carer")

- This governs the use and care of devices assigned to the parent's/carer's child (the "pupil"). This agreement covers the period from the date the device is issued to when the devise it returned to school.
- Once issued, the lPad shall become the responsibility of the parent/carer on behalf of the pupil until they return it to school.
1. The school is providing the pupil with an lPad ("the equipment") for the purpose of completing remote learning from home during this current National lockdown in January 2021.
2. This agreement sets the conditions for receiving an lPad ("the equipment") in order to work at home.
I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss
- By signing this agreement I agree to take full responsibility for the equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.
- I understand that I and the pupil are responsible for the equipment at all times.
- I understand that I must arrange for adequate insurance cover for damage or loss of the IPad. This is my responsibility; the Ipad will not be covered by school insurance cover.
- I acknowledge that I am responsible if the equipment is damaged, lost or stolen. The school does not accept liability for damage to or loss of the Ipad.
- I agree to keep the equipment in good condition and ensure it is used to support home learning.
- I will not leave the equipment unsupervised in unsecured areas.
- I will make sure my child takes the following measures to protect the device:
  - Keep the device in a secure place when not in use
  - Don't leave the device in a car or on show at home
  - Don't eat or drink around the device
  - Don't lend the device to siblings or friends
  - Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use
- I agree that my child will not carry out any activity that constitutes 'unacceptable use'.
- I agree that I am responsible for ensuring that the internet is used safely as a learning resource.
- This includes, but is not limited to the following:
  - Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
  - Any illegal conduct, or statements which are deemed to be advocating illegal activity
  - Activity which defames or disparages the school, or risks bringing the school into disrepute
  - Causing intentional damage to ICT facilities or materials
  - Using inappropriate or offensive language

4. Data protection
- I agree to take the following measures to keep the data on the device protected.
  - Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
  - Make sure my child locks the equipment if it's left inactive for a period of time
  - Do not share the equipment among family or friends

- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

5. Consent

- By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	