

Christ Church (Church of England) Infant School and Nursery



E-safety Policy

'Working together to build a strong foundation through Faith and learning'.

Agreed: February 2021

Review: February 2024

E safety

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

At Christ Church Infant School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Executive Head teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice. All staff are responsible for implementing and teaching the agreed e safety rules and lessons across the school. Staff are also responsible for ensuring that they themselves are adhering to the policy in their own technology use in school.

Writing and reviewing the e-Safety policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.

Our e-Safety policy has been agreed by the Senior Management Team and Staff.

The E-safety policy and its implementation are reviewed annually

E-Safety skills development for staff

- All members of staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
 - All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
 - All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction. (appendix C)
 - All members of staff incorporate e-Safety activities and awareness at the start of every term.
- Community use of the Internet

Community use of the Internet

- External organisations using the school's ICT facilities must adhere to the e-Safety policy.

Teaching and Learning Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Children will have at least 6 hours of e –safety specific teaching across the year in line with national guidance. One hour each half term will be taught at the start of each new computing topic.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Communications Policy Introducing the e-Safety policy to pupils

- E-Safety rules are displayed in each classroom and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson must be taught each term and at relevant points throughout e.g. during PSHE lessons//anti-bullying week/Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored. The school uses Securus software which is monitored by the JCT.

- The school is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search
- Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

Staff and the e-Safety policy

- All staff must sign the Staff AUP and a copy is kept on file. (introduced Feb 2021) (Appendix C)
- Any information downloaded must be respectful of copyright, property rights and privacy.
- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school (see laptop use policy) (Appendix F). Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Staff will also sign and agree the social media policy (Appendix B)

Parents and the e-safety policy

- All parents, when their child joins the school, will be asked to sign the AUA for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's E-safety policy.(introduced September 2021) (Appendix A)
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website. (Appendix E)
- Parents are encouraged to look at the school's e-safety policy and the acceptable use policy for students. Parents will also sign an internet permission form.

The Learning Platform and other home/school internet use

- All staff have been trained and given advice on how to effectively use SIMs, the learning platform and TEAMS.
- All children will be given a username and password to access secure resources and facilities on the learning platform and to access TEAMS. These should not be shared outside of the family.
- The school website forums and TEAMS will be regularly monitored for incidents of cyberbullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending of messages through TEAMS is monitored.
- Class teachers will monitor the use of TEAMS. Any misuse of the TEAMS messaging will be reported to the Head teacher.

The governors and the e safety policy

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning

- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator within the role of the DSL and a named governor takes responsibility for e-Safety (Lynn Percival).
- an e-Safety Policy has been written by the school, building on Wolverhampton's LA e-Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is understood and not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix A

Christ Church, Church of England Infant School Acceptable Use Policy for pupils in Key Stage One

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- ☺ always keep my passwords a secret
- ☺ only visit sites which are appropriate to my work at the time
- ☺ only use the school learning platform to store and access my school work
- ☺ not let anyone else use my learning platform log on
- ☺ only post things on the platform that I would say in class
- ☺ work in collaboration only with individuals or groups agreed by my teacher or other responsible adult
- ☺ tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- ☺ make sure all messages I send are respectful
- ☺ inform a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- ☺ do not reply to or forward any nasty message or anything which makes me feel uncomfortable
- ☺ only email people I know or those approved by a responsible adult
- ☺ only use email in school which has been provided by school
- ☺ only connect to the agreed school wireless broadband while in school
- ☺ talk to a responsible adult before joining chat rooms or networking sites
- ☺ I will inform a responsible adult if I come across anything in chat rooms or networking sites that makes me feel uncomfortable
- ☺ always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- ☺ always check with a responsible adult and my parents before I upload photographs of myself
- ☺ never meet an online friend without taking a responsible adult that I know with me

I understand:

- ☺ Using computers safely can make everyone's learning more enjoyable
- ☺ Anything I do on the computer may be seen by someone else
- ☺ Anything I put on the TEAMS Chat will have my name next to it
- ☺ Most social networking sites have a minimum joining age and it is a criminal offence to give false information e.g. lie about my age or gender
- ☺ Not everyone on line is who they say they are

I know that once I post a message, picture or any other item on the internet then it is completely out of my control.

I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

Name Date
.....

Appendix B

Christ Church, Church of England Infant School Social Media

(Facebook, Instagram, Twitter, Snapchat, etc)

All staff should ensure that they are fully aware of the following:

- References to places of work, school, telephone numbers or addresses, should not be given on websites
- No reference to roles at work, job titles or confidential information should be given.
- Colleagues should not be subjected to inappropriate or unwanted reference either in writing or photographs
- Staff should not accept 'Friend' requests from pupils present or past under the age of 16 years.
- Staff should not accept 'Friend' requests from parents of pupils at Christ Church Infant School (unless the adult is also a member of staff at this school) and should maintain a professional distance in online communications.

This guidance is to help staff become aware of the best practice when using social websites.

It is designed to ensure staff understand that the school and colleagues should not be compromised by inappropriate comments.

It will be deemed a disciplinary offence should these guidelines not be adhered to.

Should any member of staff be unsure of how to interpret these guidelines, then advice should be sought from the Head Teacher.

Appendix C

Christ Church, Church of England Infant School

Acceptable Use Agreement for the School Workforce.

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

I agree that I will:

- only use personal data securely
- implement the schools E-safety policies
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts in school
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc...
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the Headteacher
- ensure that videoconferencing is supervised appropriately for the learner's age
- pass on any examples of Internet misuse to the Headteacher
- post any supplied E-safety guidance appropriately
- think carefully about what is stored on my laptop and make efforts to store sensitive data on the school server or private area on the Learning Platform
- think carefully about what is stored on my memory stick and make every effort to send sensitive information using a secure email rather than use a memory stick

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger
- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

I confirm that I have read and understand the content of Appendix A relating to the use of online Social Networking Sites such as Facebook.

I understand that there should be no reference to the school or inappropriate sharing of information relating to pupils or staff via such sites. I understand that to do so could result in disciplinary action. All staff members accessing such sites have a duty

of responsibility to report inappropriate content relating to the school or its stakeholders to the Executive Head teacher.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Name **Date**
.....

APPENDIX D

**Christ Church Infants School
Parent internet permission form.**

Dear Parents,

Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of ICT skills, Christ Church C.E. Infant School is providing supervised access to the Internet including email within the school community.

Although there have been concerns about pupils having access to undesirable materials, we take positive steps to deal with this risk in school. The City Council operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the Council cannot be held responsible for the nature or content of materials accessed through the Internet.

I enclose a copy of the Rules for Responsible Internet Use by Pupils that we operate at Christ Church Infant School. Please complete the permission slip below to ensure your child's access to the Internet and email.

Should you wish to discuss any aspect of Internet use please do not hesitate to get in touch.

Yours sincerely

S. BLOWER
Executive Headteacher

Permission for Internet and Email Use

I give permission for access to the Internet on the terms set out in the policy and agreement enclosed.

Name of Child: Class

Date:

Signed: Parent / Guardian

Please indicate if your child has access to the following at home:

Windows pc e mail internet printer

APPENDIX E

Christ Church Infant School
TETTENHALL WOOD

PHOTO CONSENT FORM

CHILD'S NAME CLASS

I give permission for my child to have their photograph taken in school for general purposes and local/national media, including use on the school website.

Signed: Parent / Guardian

Date:

Appendix F

**Schools Laptop Agreement –
Christ Church Infant School and Nursery**



This document is an agreement between both staff and school, and shall be binding for the duration employment at the school.

General

1. The laptop shall remain the property of the school.
2. The laptop shall be retained by staff in order to exercise their professional duties.
3. The laptop shall be returned to school upon a member of staff leaving school to take up a post elsewhere and any additional software/saved data removed.

4. Staff are to take proper care of the laptop at all times.
5. Staff shall be responsible for the security of the laptop, ensuring it is in a lockable cupboard when unattended in school and ensuring all reasonable precautions are taken when transporting the laptop.
6. Any additional software installed on the laptops is to be correctly licensed.
7. All faults are to be reported to the ICT Co-ordinator.

Use

1. The laptop shall be available for use in school.
2. Staff shall be aware of the issues relating to access to Internet sites not relevant or appropriate to their professional duties.
3. Staff shall operate Internet access with due regard to school and Wolverhampton City Council policies.
4. Staff shall use the laptop in a responsible and professional manner.
5. Staff will be expected to use the laptop for:
 - Planning
 - Delivery of lesson
 - Record Keeping
 - Analysis of assessment
 - Target Setting
 - Accessing Learning Platform
 - Other professional duties

Staff are responsible for the protection of data held on their laptop by ensuring that Bitlocker codes, usernames and passwords are not stored with the device.

Memory sticks should only be used if they are appropriately encrypted and password protected.

The school agrees to provide training for teachers in order to make effective use of their laptop.

..... I Agree to the terms and conditions above.

Signed

Signed on behalf of Christ Church Infant School and Nursery

.....