

Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Christ Church C of E Primary School On-line Safety Policy & ICT Acceptable Usage Agreement (AUA)2024



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Online Safety Policy & ICT Acceptable Usage Agreement (AUA)

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body

September 2023

The implementation of this Online Safety policy will be monitored by the:

Online Safety Coordinator,
Head Teacher & Senior
Leadership Team

Monitoring will take place at regular intervals:

Once a term.

Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:

Once every Governors
meeting.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:

July 2024

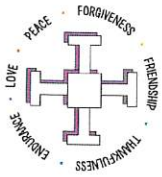
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:

LA ICT Manager, LA,
Safeguarding Officer, Police.

Rationale

As a Church School working with our local, national and international communities, Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning, stay safe and for future employment.

The Computing curriculum covers a wide range of resources including online learning and digital literacy. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom.



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Whilst exciting and beneficial both in and out of the context of education, most web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

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

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, iPads, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, smart watches and portable media players, etc).

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer) and Computing leader have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection), Childline and Local Authority Safeguarding Children Board.

This policy, supported by the school's acceptable use policies for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy.

Key staff

Head teacher - Mr. S. Davies
Computing Manager – Mr. A. Harris
Online Safety leader – Mr. A. Harris

Online Safety skills development for staff

- Our staff receive regular information and training on Online Safety issues in the form of full staff meetings and memos. Staff training related to Online Safety should take place annually.



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



- New staff receive information on the school's acceptable use policy as part of their induction through their staff handbooks and should be updated annually
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are should incorporate Online Safety activities and awareness within their curriculum areas in order to meet the requirements of the Relationships Education 2020 and Keeping Children safe in Education 2023

Governors

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governor who oversees online safety is Cllr Lee Jeavons

All governors will:

- Ensure that they have read and understand this policy
- Ensure they have had training on a regular basis about online safety

Communicating the school Online Safety messages

- Online Safety rules will be posted in all rooms and discussed with the pupils at the start of each year/lesson.
- Pupils will be informed that network and Internet use will be monitored on all devices
- Online Safety posters will be prominently displayed throughout school.

Online Safety in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety. We regularly monitor and assess our pupils' understanding of Online Safety.

- The school provides opportunities within a range of curriculum areas including using Project Evolve and to teach about Internet Safety (in accordance with the medium-term planning.) This include the 8 strands from Education for a connected world and associated objectives.
- Educating pupils on the skills needed when they may encounter the dangers of technologies outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and peer to peer abuse and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Password Security

Password security is essential for staff and pupils. Staff can access and use pupil data. Staff have access to this through Administrator Rights on the school's network. KS2 have chrome books and pupils all have personalised logins for these for use on the Chromebook. These passwords are personalised for each pupil. KS1 pupils have access to iPads, these don't require a login. They are filtered through the internet provision, the children are taught about what to do with online safety issues and fully actively supervised for the time they use them.

Staff and pupils are regularly reminded of the need for password security. Passwords for staff are changed on a regular basis at least annually and reminders are given about enforcing password policies. The pupil passwords are kept on a secure file which password protected and on the school network.

Data Security

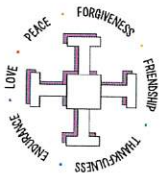
The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher. Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/pupil data. The school adheres to the General Data Protection Regulations. The Data manager is Mr. S. Davies. More information related to this can be found in the Data Protection policy.

Data management means that memory sticks should not carry personal data including full names, if memory sticks are used then they should be encrypted. Alternative access to the school network is through the CC4 VPN and staff can use Google Drive as well.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected, it will be followed up.

- All staff must read and agree to the 'Acceptable Usage Agreement' before using any school device.
- Staff will preview all sites before use. The use of the internet should be pre-planned. This will be shared with pupils through QR codes, Google classroom or given links



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



- Raw image /video searches are discouraged when working with pupils unless using Swiggle (<https://swiggle.org.uk/>) as a child friendly search engine. Using Google classroom including Docs and Slides, pupils will be encouraged to use search tool to insert images.
- If Internet research is set for any work including homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites at home and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through a web filtering service, Netsweeper.
- Our school also employs some additional web monitoring - Nicola Rudge (Online Safety advisor for Walsall Children's Services).
- Staff and pupils are aware that all activity on devices can be monitored on network devices and chromebooks and explored further if required. Staff should be aware iPads cannot be monitored so a good practice approach is that the internet is filtered, children know how to report problems and staff should fully supervise all pupils whilst using these devices.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the class teacher who must inform an Online Safety co-ordinator and dealt with appropriately including logged on CPOMS and passed to the safeguarding team.
- It is the responsibility of the school, by delegation to the technical support; to ensure that anti-virus protection, filtering and monitoring software is installed and kept up to date on all school machines.
Monitoring emails are sent weekly to summarise the monitoring activity on the network and device numbers to ensure this is still active.
Filtering is tested using - <http://testfiltering.com/> is done by the ICT technician once half-termly on random devices in the school to ensure it is working correctly and a log kept for this on the network.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Computing Manager or Head teacher.
- If there are any issues related to viruses or anti-virus software, the Computing manager should be informed immediately.

Social Media

Websites, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.



Christ Church CE Primary School

'Train up a child in the way they should go and, when they are old, they will not depart from it.' Proverbs 22:6



Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones and smartwatches)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. Staff should not use these when they are in direct contact with children, during teaching time this should be locked away in a locker/cupboard. Staff may use these devices in the staff room. Smart watches should be silenced and notifications disabled while staff are teaching and working with children in order to prevent the possibility of pupils reading/seeing what is on devices.
- Pupils are not encouraged to bring personal mobile devices to school unless they are pupils in Y5/6 who walk home unaccompanied by an adult/carer. In this case the device is handed in and put away in a locked drawer or cupboard in the classroom in order to keep them safe whilst in school.
- The school is not responsible for the loss, damage or theft of any personal mobile device/phone.
- The sending of inappropriate messages between any members of the school community is not allowed. School agreed communication systems e.g. email, should be used for professional communications and no other method.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing communication

The use of email within most schools is an essential means of communication for both staff. Educationally, email can offer significant benefits including; direct written contact between schools on different projects and communication. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Some year groups have parents contacting staff members via a generic email address e.g. Year1@christchurch.walsall.sch.uk rather than using personalised email addresses.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business and all communication should be professional in tone



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus-checking attachments.
- Staff must inform the Computing manager or Head teacher if they receive an offensive e-mail.

Safe Use of Images

Taking of Images and Film

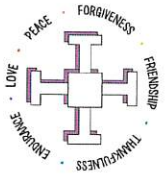
Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless in extenuating circumstances and only with agreement of head teacher.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school to record images and can download these images on the school network.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Twitter account
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)



Christ Church CE Primary School

'Train up a child in the way they should go and, when they are old, they will not depart from it.' Proverbs 22:6



This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent must be given by both parents for it to be deemed valid.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

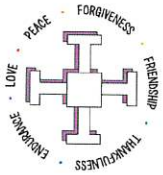
Misuse and Infringements

Complaints

- Complaints relating to Internet safety should be made to the Computing manager or Head Teacher.
- All incidents will be logged via CPOMS and followed up.
- Complaints of a child protection nature must be dealt with in accordance with schoolchild protection procedures and must be reported to the Named person (Safeguarding Officer).
- Pupils and parents will be informed of the complaints procedure which can be found on the website.

Inappropriate material (see Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Computing manager, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned as part of the curriculum and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to the internet and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school and when they change key stages.
- Parents/carers are required to decide as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to Online Safety where appropriate in the form of;
 - Information sessions
 - Posters
 - Links to further information
 - Newsletter items
- Parents will be advised that the use of social network spaces outside school are inappropriate for primary aged pupil.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites.



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Staff, Governors and visitors Computing Acceptable Use Policy (AUP)

POLICY STATEMENT

The Governing Body recognises the use of the Internet and devices as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for computing to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the school's computing systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use:

1. Not depriving pupils of the use of the equipment

and/or

2. Not interfering with the proper performance of the staff member's duties

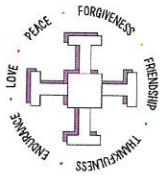
Whilst the school's devices may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the high standards of Safeguarding expected by all members of the staff.

The use of computer equipment, including laptop computers, which is on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy. Staff must remember that the use of these devices is monitored both in and out of school.

GUIDANCE ON THE USE OF SCHOOL COMPUTING FACILITIES

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to and including disciplinary action

Further guidance on the responsible use of Computing facilities are contained in the Council document "*Internet Access Policy for Schools*".



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



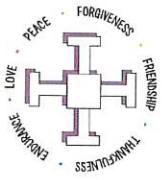
E-mail and Internet usage

The following uses of the school's devices are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. To gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it.
2. To gain access to, and/or for the publication and distribution of material promoting racial hatred.
3. For bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation.
4. For the publication and/or distribution of libellous statements or material which defames or degrades others.
5. For the publication and distribution of personal data without either consent or justification.
6. Where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination.
7. To participate in on-line gambling.
8. Where the use infringes copyright law.
9. To gain unauthorised access to internal or external computer systems (commonly known as hacking).
10. To enable or assist others to breach the Governors' expectations as set out in *this policy*.

Additionally, the following uses of school devices are not permitted and could lead to disciplinary action being taken:

1. For participation in "chain" e-mail correspondence.
2. In pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives).
3. To access devices using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.



Christ Church CE Primary School

'Train up a child in the way they should go and, when they are old, they will not depart from it.' Proverbs 22:6



4. Any other activity deemed unsuitable

Use of School Equipment/devices

Users of school equipment/devices:

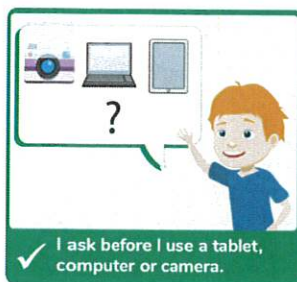
1. Must not share and must treat as confidential any passwords provided to allow access to equipment and/or beyond firewall protection boundaries.
2. Must report any known breach of password confidentiality to the Headteacher or nominated Online Safety or Computing Co-ordinator as soon as possible.
3. Must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's devices/equipment
4. Must not install software on the school's devices, including freeware and shareware, unless authorised by the school's Computing Co-ordinator.
5. Must comply with any Online Safety security procedures governing the use of systems in the school, including anti-virus measure.

Regulation of Investigatory Powers Act 2000

Ancillary to their provision of ICT facilities, the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

Acceptable Usage Policy - Pupils

EYFS





Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



KS1

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post to our blogs, use our email and other communication tools.

KS2

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash
- To help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed, and appropriate actions taken.

T	= is it true?
H	= is it helpful?
I	= is it inspiring?
N	= is it necessary?
K	= is it kind?



Christ Church CE Primary School

'Train up a child in the way they should go and,
when they are old, they will not depart from it.' Proverbs 22:6



Signed:

Head Teacher

Date: February 2024

Next Review: February 2024