



CROWTHORNE CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety & Acceptable Use Policy

Status of Policy	Date
Statutory	Statutory
Reviewed	Every 2 years
Ratified by governors	February 2026
Review date:	February 2028

Our school policies reflect our vision of

*Inspiring and enabling our school community to live life to the full,
promoting excellence and nurturing respect, honesty, compassion, resilience and collaboration.*

John 10 v 10:

Jesus said: "I have come that they might have life, and have it to the full"



CROWTHORNE CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety and Acceptable Use of Internet Policy

The E-Safety Policy relates to other policies including those for Computing, Anti-Bullying and Safeguarding and Child Protection.

The Headteacher will oversee this area, with the Computing Subject Leader, and delegate where necessary.

Our E-Safety Policy has been written by the school, building originally on the Kent E-Safety Policy and government guidance, in particular guidance within Keeping Children Safe in Education. It has been agreed by all staff and approved by governors.

Aims

Crowthorne Church of England Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, empowering us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as 'mobile phones')
- Provide learning opportunities that enable pupils to benefit from the wealth of opportunity available on line, supporting them to live life to the full, whilst also educating about the risks
- Ensure our E-safety and Acceptable Use Policy provides clear guidance to support safe access to the internet and to provide accountability measures to protect all members of our school community

How Use of Technology Supports Pupils and Staff to Flourish

Whilst this policy predominantly addresses the risks posed by the use of technology and the processes and procedures in place to monitor and reduce risk, it is also important to note the benefits of technology and how its use supports our school vision. We live in an ever-more technology-driven world and our children have never experienced life without a host of different forms of technology impacting many areas of their lives. Learning how to use technology well and in ways that enhance knowledge, well-being and opportunities is vital for our young people. The internet provides access to almost endless information, tools to support learning and personal growth and opportunities to connect and communicate with people it may not be feasible to meet in person. These aspects of technology use are beneficial for both children and staff and support our vision of enabling our school community to live life to the full, in all areas of life.

Categories of Risk

There are four key categories of risk that we address through our approach to online safety:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subject to harmful online interaction with other users, such as peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increased the likelihood of, or causes, harm, such as making, sending and receiving explicit images (eg consensual or non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online buying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

The governor who oversees online safety is Richard Farnworth.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding lead (DDSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The headteacher is the DSL at Crowthorne C of E Primary School.

The DSL and DDSL take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- The DSL will take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- The DSL will work with TSI and the Bursar to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT manager and technical support

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing DSL/TSI and the school bursar
- Following the correct procedures by adding to planning if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it in full.

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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 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. They will be 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
- Pupils will be taught how to evaluate Internet content, including a growing understanding of misinformation and 'fake news'
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon

Social networking and personal publishing

- The school will not allow access to social networking sites using the school network.
- Pupils will be taught that social network sites have age restrictions, and it is recommended that primary aged children do not have a profile on any social networking site.
- Pupils will be taught and advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when online.

Mobile Phones in School

- Pupils will only be given permission to bring their phones to school when this permission has been requested by parents from the Headteacher. Parents are requested to support their child in safe use of their phone and to check their children's phones regularly.
- Mobile phones will not be used during lessons or formal school time by pupils. They are to be handed over to the office before school and collected when school finishes. Mobile phones are not allowed on school journeys.
- These statements should be read in conjunction with the school's Mobile Phone and Smart Device Policy

E-mail

- Pupils do not routinely have access to email accounts in school
- Pupils may only use approved e-mail accounts on the school system as part of curriculum learning.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from an adult.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Managing videoconferencing & webcam use

- Videoconferencing (including the use of Teams and Zoom) should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call or meeting invite.
- Videoconferencing and webcam use will be supervised and will generally be for group lessons provided by other organisations, not for individual 1:1 conversation
- Staff using videoconferencing for training courses or meetings must ensure that sensitive information is not visible to others on the call and that all reasonable attempts are made to ensure the call is not overheard if including confidential information

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Artificial Intelligence (AI)

At the present time, children only use Artificial Intelligence (AI) tools under close supervision and in specific circumstances, usually only in Upper Key Stage Two.

Staff may use AI Chatbots (such as ChatGPT) to support with lesson planning, the creation of learning resources and the production of formal documents. However, care should be taken to ensure that any information gained from an AI facility is accurate and appropriate.

No sensitive or personal information should be inputted into any AI service.

At Crowthorne C of E Primary School we recognize that this is a fast-developing area of technology and that, whilst bringing many benefits, it also carries inherent risk.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully to minimize the risk that their image is misused. Staff will consider using group photographs rather than full-face photos of individual children

- Pupils' full names will not be used anywhere on a school Website or other non-secure on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing

Authorising Internet access

- All staff must read and sign the "Acceptable Use Policy" before using any school IT resource.
- At Early Years and Key Stage 1, access to the Internet will be closely supervised and will involve access to specific, appropriate online materials.
- Key Stage 2 pupils will often be guided to specific online resources and will be taught how to search for appropriate information
- Any person not directly employed by the school will be asked to sign an "acceptable use of school IT resources" before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material, including the filtering and monitoring package implemented by RM. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor TSI can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Examining Electronic Devices

There must always be 2 adults present.

The headteacher, and any member of the leadership team, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or Is identified in the school rules as a banned item for which a search can be carried out, and/or Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. (If the search is not urgent, they will seek advice from the headteacher / DDSL.)
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person and/or
- The pupil and/or the parent/carers refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device
- Report the incident to the DSL (or equivalent) immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Managing filtering

- The school will work with RM and TSI to ensure systems to protect pupils are continuously reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher (as Designated Safeguarding Lead) or the Deputy.
- Senior staff and RM will ensure that regular checks are made to ensure that the monitoring and filtering methods selected are appropriate, effective and reasonable.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school's safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff who manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues. RM reports will be sent to the Headteacher and / or Bursar.
- Staff will promote the use of a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to School E-Safety in newsletters, and in the additional Knowsley Online Safety Newsletters.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents will be invited to learn about e-safety through parents information sessions which will be held at regular intervals and appropriate e-safety information will be sent home when available.

Appendices

1. Pupil Guidelines for Internet Use
2. E-Safety Rules
3. Guidelines for Managing Incidents

CROWTHORNE CHURCH OF ENGLAND PRIMARY SCHOOL

Pupil Guidelines for Internet Use

General

Pupils are responsible for good behaviour on the Internet, just as they are in the classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.

Computer storage areas will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers will always be private.

During school, teachers will guide pupils towards appropriate materials. Outside school, families will bear responsibility for such guidance, as they must also exercise with information sources such as television, films, radio and other potentially offensive media.

The following are not permitted:

1. Sending or displaying offensive pictures or messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords.
7. Trespassing in others' work folders, work or files.
8. Intentionally wasting limited resources.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with the school's Behaviour Policy on inappropriate language or behaviour.
3. When applicable, the police or local authorities may be involved.

Adapted from National Association for Co-ordinators and Teachers of Computing.

APPENDIX TWO

CROWTHORNE CHURCH OF ENGLAND SCHOOL

E-Safety Rules

- Ask permission before using the internet
- Tell a trusted adult if you see anything that makes you feel uncomfortable
- Immediately close any webpage that you are uncomfortable with
- Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details
- Make sure that when using any sites that involve communication with others, privacy settings are checked so that not just anyone can see your page/photos/information
- Only contact people that you have actually met in the real world
- Never arrange to meet someone that you have only met on the internet
- Only use a webcam with people you know – Always ask an adult before using the camera function on a device
- Think very carefully about any pictures that you post online
- Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult
- Only open e-mails from people that you know
- Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as <http://www.askforkids.com>

CROWTHORNE CHURCH OF ENGLAND SCHOOL

MANAGING INCIDENTS

The e-safety lead / DSL will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the designated Safeguarding Lead (or the Deputy)
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident on CPOMS
6. Identify support for the child, young person or vulnerable adult

Has someone been bullied?

1. Report to the designated Safeguarding Lead (or the Deputy)
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Cyberbullying

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

School will explain to pupils that this behavior is inappropriate and that, where appropriate, relevant people and professionals will be contacted (which may include the police and parents).

Has someone made malicious/threatening comments? (child/young person/vulnerable adult or organisation staff/volunteer)

1. Report to the DSL or Deputy
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the DSL or Deputy
2. If illegal do not log off the computer but disconnect from the electricity supply to the monitor and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website (RM)
8. Log the incident (CPOMS)
9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

1. Refer to the Headteacher.
2. If the concern is about the Headteacher, refer to the Chair of Governors.

All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Note: Please refer to Appendix F for a summary of what constitutes inappropriate and illegal acts involving the internet and electronic communication technologies. Further advice and guidance is shown below.

Children and Young People

To discuss an e-safety concern involving a child or young person, please contact Children's Social Care & Duty Team 01344 352020

Vulnerable Adults

To discuss an e-safety concern involving a vulnerable adult, please contact Adult Social Care and Health Community Response and Re-enablement Team on 01344 352000

For professional advice, contact the UK Safer Internet Centre's Helpline on helpline@saferinternet.org.uk or 0844 381 4772.

To request an e-safety presentation for parents/carers or for children, young people and vulnerable adults, please contact Childnet on kidsmart@childnet.com



CROWTHORNE CHURCH OF ENGLAND SCHOOL

ACCEPTABLE USE POLICY (AUP) FOR STAFF AND VOLUNTEERS

Please sign and return to the School Office

This covers use of digital technologies in the organisation i.e. e-mail, internet, and network resources, learning platforms, software, mobile technologies, equipment and systems. Any questions you may have regarding e-safety or the acceptable use of the IT facilities in school should be directed to Emily Hicks (Head Teacher / Designated Safeguarding Lead) or to the Computing Subject Leader, Karen Smith. TSI is the network manager.

By signing this form, you agree to the following conditions:

- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use an e-mail account allocated by the school, for school business.
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the headteacher
- I will not allow unauthorised individuals to access e-mail / internet / networks of systems.
- I will ensure that all my login credentials (including passwords) are only shared with the IT Support and Headteacher.
- I will ensure that all laptops (or other devices) are left locked if I am no longer in the room and that e-mails are never displayed on an Interactive whiteboard screen or via a projector
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed. I will speak to IT support if I find software on the Internet I wish to have on my laptop.
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs, including Facebook and Twitter, etc. that I create or actively contribute to are not confused with my professional role.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.

- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification.
- I understand that if I use a personal device in school, I must comply with the same rules and any internet access that will be viewed by pupils must be through the school's WiFi and not a mobile hotspot or any other personal means of connection
- I will not allow students to use a laptop / whiteboard that have been assigned to me unless under close supervision. I understand that I will not loan my laptop to family members or friends.
- I will bring my laptop to work on a daily basis.
- If I no longer work at the school I will return my laptop to the School Bursar with all other electronic devices.
- Visitors to the school who require access to the internet can only do so with the permission of those named above.
- I will not use the IT facilities in school for personal reasons at any time when I am not on a timetabled break, including during directed time after school.
- Any photos taken will be transferred to the school network and then deleted from the individual device.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.
- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with the Acceptable Use Policy (AUP) could lead to disciplinary action.

Social Networking Sites

- At home, I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. I will not use these forums to make any comments in relation to the school, colleagues or students or to post any information relating to the school including photographs.
- I will not access social networking sites such as Facebook or MySpace while using the IT facilities in school or on my school laptop in or out of school.

- I will not accept 'Friend Requests' from the parents of pupils unless they are a personal friend outside of school; in this case, I will declare this relationship to the Headteacher in order to protect myself
- I will not share information about the school in internet forums as it is unacceptable and can bring the school and / or the local authority into disrepute and put children at risk.
- If I see or become aware of inappropriate information about staff or children through conversations with colleagues, parents or partners, I understand that I have a responsibility to alert the school. I will keep this information confidential in line with the Data Protection Act and within the school's safeguarding policy. However, there may be times when I am required to disclose information to an appropriate authority such as the Police or Children's Social Care. In such cases, I can seek advice from the school's safeguarding officer or Local Authority HR.

CROWTHORNE CHURCH OF ENGLAND SCHOOL

ACCEPTABLE USE POLICY FOR STAFF AND VOLUNTEERS

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (AUP).

I agree to abide by the school's most recent Acceptable Use Policy (AUP).

Signature Date

Full Name (print)

Job title

OrganisationCrowthorne Church of England School

Authorised Signature/Manager

I approve this user to be set up

Signature Date

Full Name Emily Hicks
Job Title Headteacher



CROWTHORNE CHURCH OF ENGLAND SCHOOL



ACCEPTABLE USE POLICY (AUP) FOR CHILDREN (EYFS and KS1)



These rules are to keep me and others safe and to make sure that the school's IT systems are used in the right way.



When I use the school's IT systems (like computers and tablets) and use the internet in school, I will always:

- Ask a teacher or adult before using IT equipment
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not do things that might upset them
- Look after the school IT equipment carefully and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Only access my own files on the school network, not those of other children or adults
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I understand that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed _____

Name _____ Year _____

Parent/carer signature: _____ Date _____



CROWTHORNE CHURCH OF ENGLAND SCHOOL



ACCEPTABLE USE POLICY (AUP) FOR CHILDREN (KS2)



These rules are to keep me and others safe and to make sure that the school's IT systems are used appropriately.



When I use the school's IT systems (like computers and tablets) and use the internet in school, I will always:

Always use the school's ICT systems and the internet responsibly and for educational purposes only

- Only use school IT equipment when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or appropriate adult) immediately if I find any material which might upset or harm me or others
- Save my work on the school system and only access my own files, not those of another child or adult
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites - including social networking sites, chat rooms and gaming sites - unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Years 5 and 6 only: If I bring a personal mobile phone or other personal electronic device into school:

- I will only do so if my parent/carer has requested permission and this has been granted
- I will not use it during lessons, clubs or other activities organised by the school; all devices should be handed in to the school office at the start of the day and collected at the end of the day
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I understand that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed _____

Name _____ Year _____

Parent/carer signature: _____ Date _____