CHEW STOKE CHURCH SCHOOL

E-Safety Policy

This policy is written with reference to the Christian Foundation of the school.
'Confident in Learning, Caring in Life'
Our vision has been inspired by Luke 10:27

This policy should be taken and used as part of Chew Stoke Church School's overall strategy and implemented within the context of our aims and values as a Church of England School.

1) RATIONALE

New technologies have become integral to the lives of children in our community, both within school and in their lives outside. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this safety policy is used in conjunction with other school policies (e.g. pupil behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2) ROLES AND RESPONSIBILITIES

Governors

Approve and review the effectiveness of the E-Safety policy and acceptable use policies. A member of the Governing Body (Personnel Committee) has taken on the role of E-Safety Governor which includes:

- regular meetings with the e-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors where necessary

Headteacher
The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. The Headteacher is responsible for ensuring that all staff receive appropriate training to enable them to carry out their safety roles and to train other colleagues. The Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or a pupil (see SWGfL flow chart on dealing with e-safety incidents in the section on "Responding to Incidents of Misuse" and relevant Local Authority disciplinary procedures).

E-Safety Coordinator (Elliott Jones)
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors (curriculum committee)
- reports regularly to Senior Management Team

Technical Support Staff
The ICT Technician is responsible for ensuring:
- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he keeps up to date with E-safety technical information in order to effectively carry out his E-safety role and to inform and update others as relevant

Teachers and Support Staff
They are responsible for ensuring that:
- they have an up to date awareness of E-safety matters and of the current school safety policy and practices and have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator/Headteacher
- all digital communication with pupils is on a professional level and only carried out using official school systems
- E-safety issues are explicitly and regularly taught in the curriculum
- pupils understand and follow the school E-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons
- they are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils
Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at Key Stage 1 it is expected that parents sign on behalf of the children).
Pupils need to:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Parents
Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, information on the school's website and sending out information about national or local E-safety campaigns or literature. Parents are responsible for:

- endorsing (by signature for KS1 pupils) the Pupil Acceptable Use Policy
- encourage their child to follow acceptable use rules at home
- establishing appropriate filtering systems that their children use
- discussing E-Safety issues with their child(ren) and monitor their use of ICT systems (including mobile phones and games devices)
- keeping up to date with issues through school updates and attendance at events

Visitors and Community Users
All visitors and community users must sign and follow the AUP before being provided with access to school systems.

3) TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING
The school will be responsible for ensuring that the school infrastructure/network is safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities.

- The school ICT systems will be managed in ways that ensure that the school meets the E-safety technical requirements outlined in the SWGfL Security policy and Acceptable Usage Policy and any relevant LA e-safety guidance
- There will be regular reviews and audits of the safety and security of the school's ICT systems
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password by the ICT technician
- The master passwords are also available to the Headteacher and secured safely in the school safe.

4) CURRICULUM
E-safety should be a focus in all areas of the curriculum and staff should reinforce safety messages in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for

their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites they visit. It is accepted that from time to time, for good educational reasons, children may need to research topics that would normally result in internet searches being blocked (eg racism, drugs, discrimination). In such a situation, staff can request that the Subject Leader or ICT technician temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Staff must realise that at least 2 weeks' notice needs to be given in these circumstances, as well as being particularly vigilant during teaching time if some sites have become 'non-filtered'. Pupils should be taught in all lessons to be aware of the materials / content they access on-line and be guided to validate the accuracy of information. Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5. USE OF PHOTOGRAPHIC AND VIDEO IMAGES

Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital/video images (with parental consent) to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes without permission from the Headteacher.
- Care should be taken when taking digital/video images that the pupils are appropriately dressed and are not participating in activities that might bring the school into disrepute.
- Photographs published on the website will be selected carefully.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of pupils are published (via the blanket permission form).

6. DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- *Fairly and lawfully processed*
- *Processed for limited purposes*
- *Adequate, relevant and not excessive*
- *Accurate*
- *Kept no longer than is necessary*
- *Processed in accordance with the data subject's rights*
- *Secure*
- *Only transferred to others with adequate protection*

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

7. SOCIAL NETWORKING

The Governing Body of Chew Stoke Church School recognises that employees have the right to access social networking websites for personal communications in their leisure time. Social networking sites allow users to build on-line profiles and share information; however users are reminded that information loaded onto such sites may be viewed by others, therefore information you do not wish others to view should not be uploaded in such a public domain. Users are also to bear in mind that information they share through social networking applications (even if they are using personal equipment) are still subject to copyright, data protection and Freedom of information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. The Governing Body of Chew Stoke Church School is committed to ensuring that all staff are aware of their responsibilities in connection with the use of social networking sites. All staff are expected to keep a professional distance from pupils and there should be a clear separation of the private social lives of staff and that of pupils. It is important that staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. However, it is also important to ensure that this is balanced with the school's duty to safeguard children, the reputation and ethos of the school, the wider community and the LA.

Guidance and Regulation for the use of Social Networking Sites

- Staff that use social networking sites should behave responsibly and professionally at all times
- Staff are responsible for all contents/comments on their own site
- Staff need to ensure that security settings are set to the highest possible level
- Staff must adhere to the school's own usage policy in relation to accessing social networking sites for personal use
- Staff **must not** accept pupils as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations
- Staff are strongly advised not to be friends with recent pupils. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking
- Staff should not place inappropriate photographs on any social network space
- Staff should not post indecent remarks
- If a member of staff receives a message on his/her social networking profile that they think could be from a pupil they must report it to the Headteacher and contact the internet service or social networking provider so that they can investigate and take the appropriate action
- Staff should not write about their place of work, their colleagues or pupils; should a member of staff do so, he/she will be in breach of this policy and potentially subject to disciplinary action
- Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act
- Staff must not disclose any information about the school that is not yet in the public arena
- In no circumstances should staff post photographs of pupils
- Staff should not make defamatory remarks about the school/colleagues/pupils or post anything that could potentially bring the school into disrepute
- Staff should not disclose confidential information relating to his/her employment at the school
- Care should be taken to avoid using language which could be deemed as offensive and inappropriate to others
- Staff need to be aware that the Governing Body will take seriously any occasion where guidelines are not followed and may result in disciplinary proceedings

8. COMMUNICATIONS TECHNOLOGY

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks /disadvantages:

Communication Technologies	Current policy for staff	Current policy for pupils
Mobile phones may be brought to school	Yes	For older (Y5/Y6) children only, and where there is a reasonable need. All phones should be handed to the class teacher to store securely until the end of the day
Use of mobile phones in lessons or directed work time	Not for communication* or photographing, or pleasure - but may be used as a watch, calculator, music player, stopwatch etc. *unless a genuine emergency	No
Use of mobile phones in social time	Yes (but see notes below)	No
Taking photos on mobile phones or PDAs etc	No	No
Use of personal email addresses in school	Yes but only in social time (see section 9 below)	No
Use of school email for personal emails	No	No
Use of chat rooms and facilities	No*	No
Use of instant messaging	No*	No
Use of social networking sites	No*	No
Use of blogs	No*	No

*this includes the use on personal devices at all times in school

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Headteacher – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents /carers (email, text message etc.) must be professional in tone and content

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

Users shall not visit internet sites, make, post, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion of illegal acts (e.g. under child protection, obscenity, misuse, fraud)
- Adult material that potentially breaches the Obscene Publications Act in the UK

- Criminally racist material
- Pornography
- Promotion of any kind of discrimination or racial/religious hatred
- Threatening behaviour (including the promotion of violence or mental harm)
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Uploading, downloading or transmitting commercial software or copyrighted materials without the necessary licensing permissions
- On-line gaming or gambling
- File sharing
- Use of social networking sites
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential information

9. USE OF EMAIL

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer. When using e-mail, pupils and staff should:

- Not access personal emails in school using school equipment unless it is specifically related to school business. Staff must not communicate with pupils via email in any circumstance. Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account. In these circumstances the school email system must be used.
- Be aware that e-mail is not a secure form of communication and therefore staff should not send ANY personal information via email unless it is by using the school email system to another similar system
- Should not attach large files
- Must not forward e-mail messages onto others unless the sender's permission is first obtained
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Pupils will be allocated a class email account for their use in school. Pupils are not permitted to access personal email accounts without the permission of the Headteacher.
- Communication between staff and all members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to the Headteacher immediately.

10. CYBERBULLYING

Cyberbullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members

and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, or menacing and threatening communications.
There are many types of cyber-bullying including:
1. **Text messages** —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
2. **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
3. **Mobile phone calls** — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
4. **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
5. **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based chatroom.
6. **Instant messaging** (IM) — unpleasant messages sent while the user conducts real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat
7. **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo and MySpace.
The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Preventing Cyberbullying
It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our E-safety curriculum. They should:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them
- Know what to do if they or someone they know are being cyber bullied.
- Report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on **www.kidscape.org** and **www.wiredsafety.org**

11. ENLISTING PARENTS' SUPPORT

We believe that it is essential for parents/carers to be fully involved with promoting E-safety both in and outside of school. We regularly seek to raise the profile of E-safety with parents and carers and aim to promote a wide understanding of the benefits related to ICT and associated risks.
The school disseminates information to parents relating to E-safety where appropriate via:

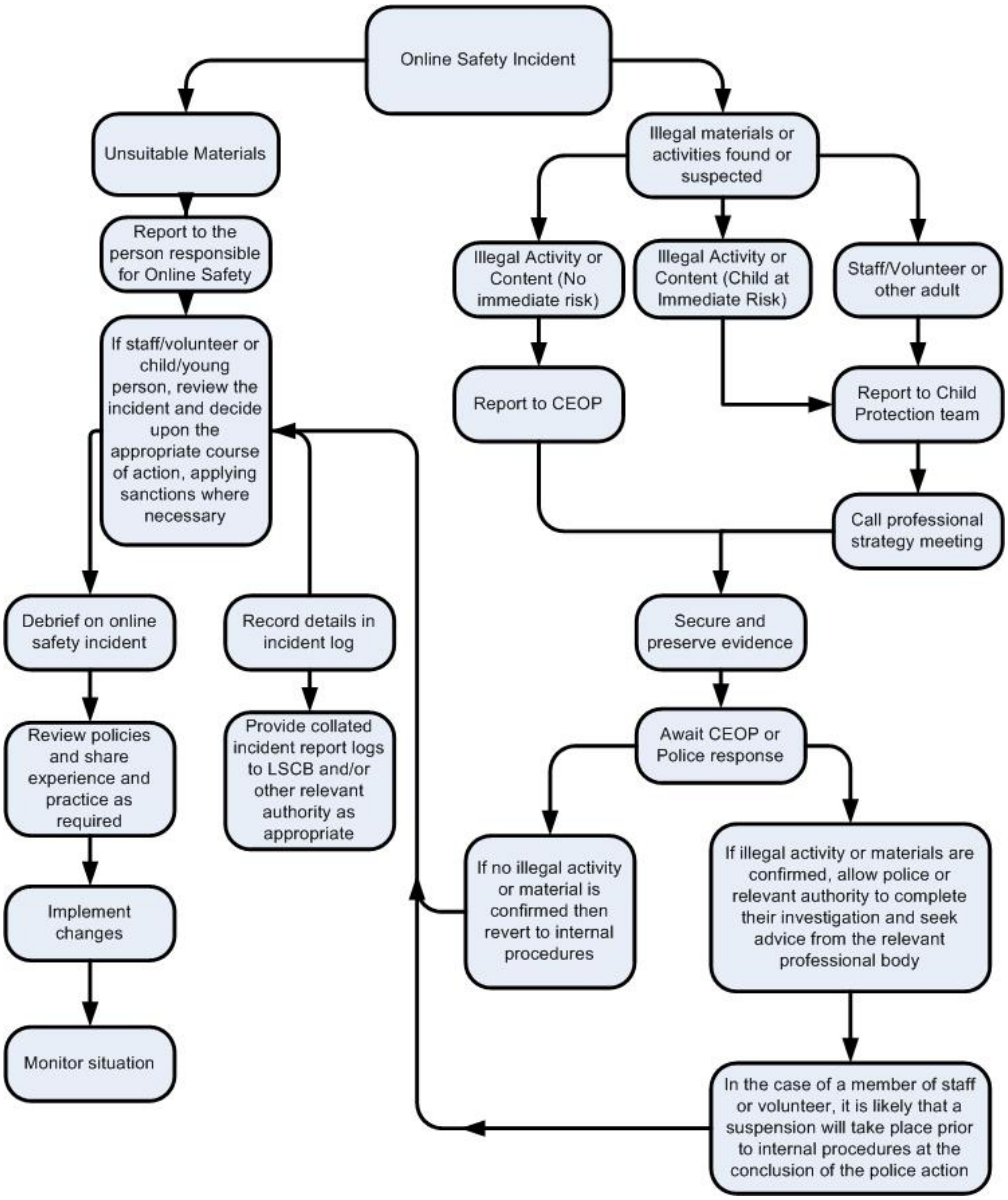
- Information via Newsletters and Curriculum Newsletters
- Posters
- Website postings
- E-Safety training events

Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendix 2).
Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website) via the blanket permission slip.

12. RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the case of a pupil, such behaviour will be referred to the Headteacher

immediately and may result in fixed-term or permanent exclusion. In the case of staff, such behaviour may result in disciplinary proceedings being started, and could lead to dismissal.
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Chew Stoke Church School will deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Incidents of misuse will be dealt with through normal disciplinary procedures.

This policy should be read in connection with all other policies, but with particular reference to:
Confidentiality Policy, Anti-Bullying Policy, Child Protection Policy, Pupil Behaviour Policy, ICT Acceptable Use Policy for Staff and Volunteers.

This policy was approved in September 2022. **Review date: January 2024**

CHEW STOKE CHURCH SCHOOL SAFETY INCIDENT LOG

Details of ALL E-Safety incidents must be reported to the Headteacher who will formally record the incident. This incident log will be monitored by the SLT as well as the governor with responsibility for E-Safety. Any incidents involving Cyberbullying should be recorded on the bullying and racist incident record form

Date & time	Name of pupil or staff	Room and device number	Details of incident (including evidence)	Actions and reasons

CHEW STOKE CHURCH SCHOOL
ACCEPTABLE USE OF ICT – PUPIL

The rules below apply to children using ICT equipment in school and the schools electronic systems. These rules will be regularly explained to the children and age appropriate language will be used. Access will only be given to pupils who have signed this form and returned it, for children in Key Stage 1 it is expected a parent will sign for their child.

I will only use ICT in school for school purposes.

I will only use my class e-mail address when e-mailing.

I will only open e-mail attachments from people I know, or who my teacher has approved.

I will not tell other people my ICT passwords.

I will only open/delete my own files.

I will not bring software, CDs or ICT equipment into school without permission.

I will only use the Internet after being given permission from a teacher.

I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.

I will not give out my own details such as my name, phone number or home address.

I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Pupil signature……..... (Parents signature in the case of a Key Stage 1 pupil)

Print name……

Date…….

Chew Stoke Church School - Staff and Volunteer ICT Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is minimal risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VPN etc) out of school
- I understand that the school ICT systems are intended for educational and professional use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials with the exception of agreed SWGFL proxy bypass.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
  I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted or password protected.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date