Chilham St Mary's CE Primary School

ACCEPTABLE USE (AUP) POLICY

Policy agreed: September 2023
Policy review: September 2026

We are a diverse, loving community, committed to providing firm foundations built on God's love and forgiveness for all. Within our family of learners, guided by Jesus' example, we nurture and encourage every individual to have the confidence to achieve their own potential, now and in the future.

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

(This policy should be read in conjunction with Chilham St Mary's CE Primary School E Safety Safety Policy)

Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world, as would be applied to the real world. Increasingly, children are accessing material through online sources (some of which may not be age appropriate). It is, therefore essential to address this and encourage a lifestyle which incorporates a healthy balance of time spent using technology and knowing what is appropriate for their age range.

This policy, supported by Acceptable Use Policies for staff, Governors, visitors and pupils exists to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks.

The Technologies

At Chilham St Mary's CEP School we understand that ICT has an increasing role in the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, in many cases, used outside of school, by the children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Gaming sites
- Text messaging and picture messaging
- Video calls

- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smart phones and tablets.

Whole School Approach to the safe use of ICT

At Chilham St Mary's CE Primary School, creating a safe ICT learning environment includes three main elements:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A progressive online safety education programme that is taught across the school involving pupils, staff and parents.

Staff Responsibilities

Online Safety is recognised as an essential aspect of teaching and learning across the school. We aim to embed safe practices into the culture of the school to allow children to feel, act and respond safely when using ICT.

All staff are responsible for teaching the children skills to use ICT appropriately. The staff will be expected to discuss online safety issues before the use of any form of technology, in all areas of the curriculum. Staff are encouraged to create a 'talking culture' in order to address any online safety issues which may arise in the classroom or around the school on a daily basis.

All members of staff are also responsible for ensuring the children know and understand the school rules regarding our use of the Internet and practice these when using the Internet. Our school Online Safety Coordinator is Neil Mankelow. , the Headteacher and Designated Safeguarding Lead (DSL) has overall responsibility for online safety. Chilham St Mary's CE Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Online Safety coordinator ensures they are up to date with online safety issues and guidance through liaison with staff members and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 Safe. The Online Safety coordinator ensures the Head Teacher, Senior Team and Governors are updated when needed.

Staff Awareness

- All staff receive regular information and training on online safety issues in the form of in-house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.

- All staff are made aware and reminded 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.
- Online safety records of concern are completed by staff as soon as incidents occur and are reported directly to the DSL (see appendix 7).
- All staff are expected to refer to school rules and online safety guidelines throughout their learning through ICT.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviour in their classroom, following school Online Safety procedures. These behaviours are summarised in the AUP appendices which must be signed and returned before use of technologies in the school.

Internet:

- Chilham St Mary's CEP School uses a "filtered" Internet Service via EiS which will minimise the chances of pupils encountering undesirable or unsafe material.
- Staff and pupils have access to the internet through the school's fixed and mobile internet technology.
- Staff will only email school-related information using their @chilham.kent.sch.uk address and not personal accounts.
- Staff will preview any websites before recommending them to pupils.
- Staff will either provide appropriate links to websites or teach children appropriate methods of searching via the Internet.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- The CEOP Report Abuse button is available on the school website. Teachers are to make children aware of this and when it is appropriate to use it.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the Headteacher. The device and username will need to be recorded for the purpose of safety.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected to not deliberately seek out offensive materials. Should a pupil encounter any such material accidentally, they are expected to report this to the teacher who can seek advice from the Headteacher.
- Pupils are expected not to use any rude or offensive language in their online communications and contact only people they know or those the teacher has approved.
- They are taught communication etiquette in email and are expected to follow these rules. No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made, unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- A copy of the pupil online safety agreement (appendix 1) is displayed in all areas where ICT is being used (classrooms, IT suite). Pupils will be asked to sign these rules

as an agreement, ensuring the awareness of the expectations. A copy has also been sent home to parents to ensure that these key messages are reinforced at home.

Passwords:

• Children are taught to log on to the school network safely and securely using a password. They are taught about the importance of keeping their password secure and safe.
• Use a strong password (Strong passwords are usually eight characters or more containing upper and lower case letters, as well as numbers.)
• Passwords should not be written down.
• Passwords should not be shared with other children or staff.

Mobile Technology

• School iPads and laptops should always be used for school-related reasons.
• Apps will need to have been researched and approved by the adult requesting them.
• Mobile devices should not leave the school premises unless agreed by a member of the SLT.
• All devices need to be accounted for at the end of each day.
• Mobile technology such as iPads and laptops are stored in a locked trolley/ charging unit. Members of staff or children must collect and return the key for these devices before and after each use which is. The key is stored in the school office and will be handed over by a member of the office staff team.
• When devices are not being used, staff should ensure that they are returned to prevent unauthorised access.
• No personal devices belonging to staff or children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times and kept on silent. These devices should be out of sight to children.
• If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be switched off and handed into the school office. Any children not following these rules will be dealt with using the school's behaviour policy.

Data Storage

• Staff are expected to save all sensitive data onto our secure online platform Kent Learning Zone (KLZ) or onto our staff shared area on our computers.
• Removable media (USB memory sticks, pen drives, CDs, portable drives) are allowed but only for data such as planning, resourcing etc. where children's names and sensitive information are not used.
• EHCP's, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.
All staff must agree to and sign (see appendix 2).

Social Networking Sites

• Use such sites with extreme caution, being aware of the nature of what you are publishing online in relation to your professional position. Do not publish any information online which you would not want your employer to see.

• Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
• A member of staff's role in school requires a high degree of professionalism and confidentiality.
• Permission from parents to allow children to be photographed and posted on the school website must be obtained before any images are posted.

Digital Images
• Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.
• Ensure you are aware of the children whose parents/carers have not given permission for their child's image to be used in school/on the school website. An up to date copy is present the school office.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could result in criminal or civil actions being brought against you.

Providing a comprehensive online safety education to pupils and parents

Staff	• All staff working with children must share a collective responsibility to provide online safety to pupils and to promote online safety in their own actions. • Online Safety will be taught across the curriculum whenever pupils and staff are using ICT. The school uses the National Online Safety Certified School Community Membership package. • The Computing Coordinator will lead an assembly each year highlighting relevant online safety issues and promoting safe use of technologies. • When using any technological devices to support learning in class, members of staff will acknowledge the school's online safety rules where appropriate and remind pupils how to report a problem if any were to arise. • Staff will encourage positive and responsible technology use by using praise and reward systems for pupils who demonstrate a consistent, clear understanding of online safety. • The school website will be updated regularly with relevant e-safety resources for parents and pupils.
Pupils	• Online Safety will be taught as an individual lesson once a term apart from Term 3, where all pupils will engage with 'Safer Internet Day'. Within these lessons pupils will be taught how to assess and manage online risk for themselves and will have a comprehensive understanding of what to do if an issue arises.

	• During Online Safety sessions pupils will also be invited to discuss strategies for the school community's online safety and how their views can support it. • Pupils will know where to find the online safety rules in their classroom and will have a clear understanding of them.
Parents	• Staff will remind parents of the online safety rules throughout the year. This will be through letters, workshops, open afternoons and meetings. • During at least one open afternoon a year, pupils will have the opportunity to educate parents through various classroom activities. • During online safety workshops parents will be invited to discuss and develop the provision of online safety at home and within the school community.

Maintaining the security of the school IT Network
EIS Kent and SNS (external IT technician) maintain the security of the school network and are responsible for checking on a regular basis that the virus protection is up to date on all technologies. However, it is also the responsibility of the IT users to uphold the security and integrity of the network.

Complaints procedure
Online safety is a high priority at Chilham St Mary's CE Primary School, therefore any complaints or concerns relating to online safety are made by a member of staff, child, parent/carer then they will be considered and prompt action will be taken.

Complaints should be addressed to the Headteacher who will undertake immediate action to investigate and liaise with the leadership team; including the designated safeguarding lead and members directly involved in the issue raised.

Incidents of online safety concern will be recorded using a Record of Concern Pro-forma (appendix 7) and reported to the school's DSL Lead (or Deputy DSL) in accordance with the school's Child Protection Policy. Any complaints of cyberbullying are dealt with in accordance to the school's Anti-Bullying Policy.

Monitoring
The Headteacher or any other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time, without any prior warning.

Monitoring may include: intercepting, accessing, inspecting, recording and disclosure of telephone calls, e-mails, instant messaging, internet/intranet usage and any other electronic communications involving employees without prior consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

Breaches of Policy
Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report
All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Lead- Rebecca Dolan. In her absence it must be reported to Vanessa Robinson or Chloe Arnold.

Chilham St Mary's CE Primary School

ICT Acceptable Use Policy (AUP) for pupils for use at home and at school
Our Charter for Good Online Behaviour

I promise – to only use the school computers and technologies for schoolwork or homework (during school time) that the teacher has asked me to do.

I promise – not to look for or show other people things that may be upsetting.

I promise – to show respect for the work that other people have done.

I will not – damage the ICT equipment, if I accidentally damage something I will tell an adult.

I will not – waste resources that are limited.

I will not – share any passwords with anyone. If I forget my password, I will let my teacher know.

I will not – share any personal information online with anyone; including my home address, phone number or any pictures of myself or others.

I will not – use other people's work or pictures without permission to do so.

I will not – use other people's usernames or passwords.

I will not – arrange to meet anyone who I have only met on the Internet.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let an adult know if anyone asks me for personal information.

I will – turn the screen off and tell my teacher or an appropriate adult straight away, if I see anything I am unhappy with.

I will – let my teacher or parent know if anyone says or does anything to me that is hurtful or upsets me, makes me feel worried or uncomfortable.

I will – let my teacher know if I see bad language or unpleasant pictures on the internet.

I will – be respectful to everybody online; I will treat everybody the way I want to be treated.

I will – ask permission from a member of staff before using the Internet.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home. I will always be myself on the Internet and not try to be someone else.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Pupils Name:_____

Signed (Parent/Carer):_____ **Date:** _____

Signed (Pupil): _____ **Date:** _____

Love Trust Respect Honesty Forgiveness Perseverance

Chilham St Mary's CE Primary School

ICT Acceptable use policy for staff

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

- Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected. As a school, we use EIS Kent Learning Zone. All members of staff have a personal login to KLZ and therefore all documents and data that contain any personal details and information must be saved within the hosted directory. If staff use a memory stick or CD, this must not contain any personal or identifiable data.
- Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.

7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the School Learning Platform (KLZ) to upload any work documents and files in a password protected environment.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media and the supervision of pupils within the classroom and other working spaces. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead (Rebecca Dolan).

11. If it is necessary to bring my own personal devices into school, these will only be used during non-contact time, without pupils. Mobile phones will be out of sight and switched to silent at all times during the school day.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Headteacher (Rebecca Dolan) as soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels, such as a school provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Online Safety/Social Media policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school code of conduct/behaviour policy and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Headteacher.

18. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Chilham St Mary's CEP School Staff Acceptable Use Policy.

Print name: _____

Signed: _____ **Date**: _____

Chilham St Mary's CE Primary School

Visitors and Volunteer ICT Acceptable use policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.

2. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the headteacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the headteacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Rebecca Dolan) as soon as possible.

10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Chilham St Mary's CEP School Visitor/Volunteer Acceptable Use Policy.

Print name: _____

Signed: _____ **Date**: _____

Chilham St Mary's CE Primary School

WIFI Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school community and allows access for education use only.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

3. The use of ICT devices falls under Chilham St Mary's CE Primary School's Acceptable Use Policy, online safety policy and behaviour policy which all pupils/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school's wireless service is password protected however; the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.
12. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Rebecca Dolan) as soon as possible.
15. If I have any queries or questions regarding safe behaviour online, I will discuss them with the headteacher.
16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Chilham St Mary's CEP School WIFI Acceptable Use Policy.

Print name: _____

Signed: _____ **Date**: _____

Chilham St Mary's CE Primary School

PTA/Committee Social Networking Acceptable Use Policy

For parents/volunteers running official social media accounts, for example PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour online, I will support the school's approach to online safety. I am aware that Classlist and Whatsapp are public and global communication tools and any content posted may reflect on the school, its reputation and services.

2. I will not use Classlist or Whatsapp to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the headteacher.
    - The headteacher retains the right to remove or approve content posted on behalf of the school.
    - Where it believes unauthorised and/or inappropriate use of Classlist or Whatsapp or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - I will not use images or videos which include any members of the school community.

6. I will promote online safety in the use of (Classlist and Whatsapp) and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

7. I will set up a specific account/profile to administrate the site and I will use a strong password to secure the account.
    - The Headteacher will have full admin rights to the account.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used. I will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Headteacher immediately.

10. I will ensure that Classlist and Whatsapp are moderated on a regular basis as agreed with the Headteacher.

11. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media.
    - I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

12. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the the headteacher.

I have read, understood and agree to comply with Chilham St Mary's CEP School PTA/Committee Social Networking Acceptable Use Policy.

Print name: _____

Signed: _____ **Date**: _____

Chilham St Mary's CE Primary School

Official Social Networking Acceptable Use Policy for Staff

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that WhatsApp is a public and global communication tool and that any content posted may reflect on the school, its reputation and services.

2. I will not use the staff WhatsApp group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the headteacher or the deputy DSL. The headteacher retains the right to remove or approve content posted on behalf of the school.

4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - I will not use images or videos which include current or past pupils of Chilham St Mary's CE Primary School.

6. I will promote online safety in the use of the staff WhatsApp group and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the Designated Safeguarding Lead/headteacher prior to use.

7. I will not set up additional staff groups. The staff group administrator is Rebecca Dolan.
    - The school Designated Safeguarding Lead and/or headteacher will have full admin rights to the group account.

8. Where it believes unauthorised and/or inappropriate use of the staff WhatsApp group or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the headteacher and/or Designated Safeguarding Lead urgently.

11. The administrator will ensure that the group is moderated on a regular basis as agreed with the school Deputy Designated Safeguarding Leads.

12. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

13. If I have any queries or questions regarding safe and acceptable practice online I will raise them with the headteacher.

I have read, understood and agree to comply with Chilham St Mary's CEP School Official Social Networking Acceptable Use Policy for Staff

Print name: _____

Signed: _____ **Date**: _____

Online Safety Record of Concern

<table>
<tr><td>Name of child:</td><td colspan="2"></td></tr>
<tr><td>Date of Birth:</td><td colspan="2"></td></tr>
<tr><td>Date of incident/disclosure:</td><td colspan="2"></td></tr>
<tr><td>Names of any other Staff/Children present:</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Record any disclosure from the child using their words. Use:
- Tell
- Explain
- Describe
- Outline

To clarify/gather information.

USE NO FURTHER QUESTIONS</td><td>Who?</td><td>What?</td></tr>
<tr><td>Where?</td><td>When?</td></tr>
<tr><td>Why are you concerned about the child?</td><td colspan="2"></td></tr>
<tr><td>Detail anything you have observed and when.</td><td colspan="2"></td></tr>
<tr><td>Detail any websites/games/films the child discussed with you. Please include avatar names, online friends names where known.</td><td colspan="2"></td></tr>
</table>

What category does the disclosure best fit with?	Grooming		
	Cyberbullying		
	Misuse of Social Networking Site		
	Sexting		
	Gaming		
	Underage Films		
	Misuse of Digital Camera		
	Other (Please Specify)		
Detail anything you have heard and when.			
Detail anything you have been told, by who and when.			
Name (Print):		**Date:**	
Position		**Signature:**	