Hunton
Church of England
Primary School

Compassion, Hope, Reverence, Wisdom

Online Safety Policy 2021

Key Details

Designated Safeguarding Lead (s):

Anita Makey

Ed Ming

Vanessa Pilcher

Named Governor with lead responsibility - Moira Ensoll, Sir David Noble

Date written: February 2021 (updated in line with KSIE 2020 Sept 2020)

Date of next review: January 2022

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

Contents

Responding to an online safety concern FLOWCHART (see page 15)

1. Policy Aims

This online safety policy has been written by Hunton CEP School, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2020, Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Board procedures.

The purpose of Hunton CEP School online safety policy is to:

- Safeguard and protect all members of Hunton CEP School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.
- Ensure there is a positive approach to online safety.

Hunton CEP School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

Hunton CEP School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Hunton CEP School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

Hunton CEP School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Behaviour and Anti-bullying policy
- Acceptable Use Policies (AUP) and the Code of conduct section of Staff Handbook
- Safeguarding policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Relationships and Sex Education (RSE)

3. Monitoring and Review

Technology in this area evolves and changes rapidly. Hunton CEP School will review this policy at least annually. The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

The named governors for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. Hunton CEP School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a culture that has online safety embedded in all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety; including a staff code of conduct *and* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety and includes peer on peer abuse, gaming, use of social media and mobile technology.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training as part of induction and child protection training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date information required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (*termly)* with the governor with a lead responsibility for safeguarding *and* online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology (including social media), both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues (eg hoaxes)and how they may be experienced by the children in their care.
- Identify online safety concerns and behaviours and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the IT infrastructure / system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and deputies) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement *and* acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems and network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

Hunton CEP School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Hunton CEP School will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Ensuring age appropriate education regarding safe and responsible use precedes internet access.
- Teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- Educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- Enabling them to understand what acceptable and unacceptable online behaviour looks like.
- Preparing them to identify possible online risks and make informed decisions about how to act and respond.
- Ensuring they know how and when to seek support and report if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

Hunton CEP School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Hunton CEP School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum Hunton CEP School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

Hunton CEP School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats which will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings.
- Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

Hunton CEP School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

Hunton CEP School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. Each school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

- **Early Years Foundation Stage and Key Stage 1**
  - Access to the internet will be by adult demonstration, with access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
- **Key Stage 2**
  - Learners will use age-appropriate search engines and online tools.
  - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems. All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

Hunton CEP School governors and leaders have ensured that our schools has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate Filtering

Education broadband connectivity is provided through (*EIS*) . We all use (*Lightspeed)* which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list. We work with (*EIS*) to ensure that our filtering policy is continually reviewed.

If learners discover unsuitable sites, they will be required to:

- Turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

7.3.4 Appropriate Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- *Physical monitoring (supervision) and monitoring internet and web access (reviewing filtering information).*

If a concern is identified via monitoring approaches:

- *The DSL or deputy will respond in line with the child protection policy.*

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our information security policy

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
We require all users to:

- Use strong passwords for access into our system.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.
- Lock access to devices/systems when not in use.

7.6 Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright. Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number. The administrator account for our website will be secured with an appropriately strong password. We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, the risk assessment, acceptable use policies, codes of conduct, social media and use of personal devices and mobile phones and our Twitter Policy.

7.8 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail (including phishing emails) will be deleted, not opened, blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the Headteacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

The use of personal email addresses by staff for any official setting business is not permitted. All members of staff are provided with an email address to use for all official communication. Members of staff are encouraged to have an appropriate work life balance when responding to email.

7.8.2 Learner email

Learners will use provided email accounts for educational purposes. Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted. Whole-class or group email addresses may be used for communication outside of the setting.

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Hunton CEP School community.
The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of Hunton CEP School community are expected to engage in social media in a positive, safe and responsible manner.
All members of Hunton CEP School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control learner and staff access to social media whilst using setting provided devices and systems on site. The use of social media during setting hours for personal use is not permitted.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of Hunton CEP School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the partnership. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the setting.

Members of staff are encouraged not to identify themselves as employees of Hunton CEP School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites. Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers
All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Headteacher.

Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher. Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

8.3 Learners Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources. We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.   Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

8.4 Official Use of Social Media

Hunton CEP School official social media channel is: Twitter The PTA has an official Facebook social media site. The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Staff use setting provided email addresses to register for and manage any official social media channels. Official social media sites are suitably protected and linked to each school website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection. All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Staff expectations
Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our social media acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputy) and the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Personal Devices and Mobile Phones

Hunton CEP School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Behaviour and anti-bullying and Safeguarding. Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of Hunton CEP School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises. All members of Hunton CEP School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared. Mobile phones and personal devices are not permitted to be used in specific areas within the site such as where children are changing, toilets and swimming pools.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy. All members of Hunton CEP School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (e.g. locked in a locker/drawer) during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices when teaching, unless in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and Headteacher.

Staff will not use personal devices:

- To take photos or videos of learners and will only use work-provided equipment for this purpose.
- Directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff allegations policy. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Hunton CEP School expects learners' personal devices and mobile phones to be handed in to the main office/class teacher during a normal school day. The use of personal mobile phones or devices for a specific education purpose eg to take photographs on a day trip or residential visit may be allowed but this would need to be risk assessed and agreed by the Headteacher prior to the visit taking place. A separate acceptable use statement would need to be signed by parents / pupils prior to using a personal device or phone.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use. We will ensure appropriate information is provided to inform parents, carers and visitors of expectations of use. Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

9.5 Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required. School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff. School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10 Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. We require staff, parents, carers and learners to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team. Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headteacher will speak with Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

10.1 Concerns about learner or parent online behaviour and / or welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns and these will be recorded in line with our safeguarding policy. The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with local policies and procedures. We recognise that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies. Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary. We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy. Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer). Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

Our DSLs have accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2020.

Hunton CEP School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, upskirting (a criminal offence) and online sexual exploitation. Hunton CEP School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. We also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Hunton CEP School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children. We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

Hunton CEP School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery. We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely. If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Hunton CEP School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
Hunton CEP School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy). We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally. We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.

- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment. Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police. If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy). If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

Hunton CEP School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site. We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Hunton CEP School schools. Full details of how we will respond to cyberbullying are set out in each school's Behaviour and Anti-bullying policy.

11.5 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Hunton CEP School and will be responded to in line with existing policies, including anti-bullying and behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.6 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy. If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Responding to an Online Safety Concern Flowchart

Key Local Contacts

Designated Safeguarding Lead (s) in each school

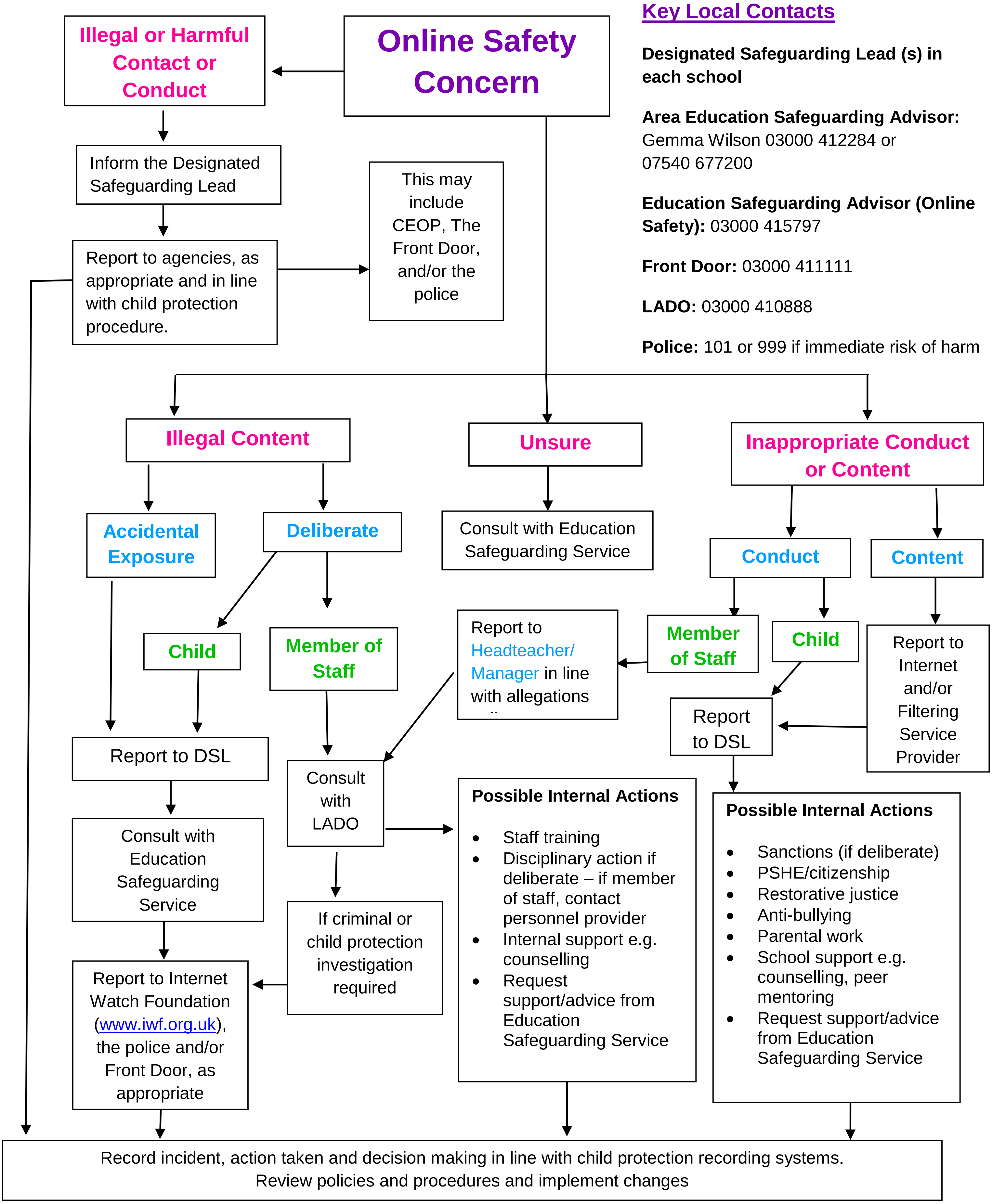
Area Education Safeguarding Advisor: Gemma Wilson 03000 412284 or 07540 677200

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, The Front Door, and/or the police

Illegal Content

Unsure

Inappropriate Conduct or Content

Accidental Exposure

Deliberate

Consult with Education Safeguarding Service

Conduct

Content

Child

Member of Staff

Report to Headteacher/ Manager in line with allegations

Member of Staff

Child

Report to Internet and/or Filtering Service Provider

Report to DSL

Consult with LADO

Report to DSL

Consult with Education Safeguarding Service

If criminal or child protection investigation required

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or Front Door, as appropriate

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

Record incident, action taken and decision making in line with child protection recording systems.
Review policies and procedures and implement changes

12. Useful Links for Educational Settings - Kent Support and Guidance for Educational Settings

Education Safeguarding Team: Rebecca Avery, Education Safeguarding Adviser (Online Protection)

Ashley Assiter, Online Safety Development Officer Tel: 03000 415797

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Hunton
Church of England
Primary School

Pupil Acceptable Use Agreement 2020-21

I understand that these rules will keep me safe and help me to be fair to others.

- I only use the internet when an adult is with me or if I have asked permission from an adult
- I only click on links and buttons when I know what they do
- I only use websites and search engines that my teacher has chosen
- I use my school computers for school work unless I have permission otherwise
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I know that if I do not follow the rules online then there will be consequences for my actions (just as there are in school and at home)
- I always credit the person or source that created any work, image or text I use
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away
- I have read and talked about these rules with my parents/carers
- If I am aware of anyone being unsafe with technology then I will report it to a teacher
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

I have read and understand these rules and agree to them.

Signed (pupil):____ Date: ______________________

I have read and understand the AUP and will support Hunton CEP School in ensuring acceptable use of the internet and school IT systems

Parent signature: _______________________________________ Date: _______________________

Hunton
Church of England
Primary School

Visitor / Volunteer / Governor Acceptable Use Policy 2020-21

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

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

- 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.

- 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.

- 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.

- 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. Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead / Headteacher.

  Governors only - 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.

- 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.

- 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.

- 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.

- 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 Designated Safeguarding Leader for my school.

- I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

- 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.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Visitor / Volunteer / Governor Acceptable Use Policy.

Signed: ……………………….... Print Name: …………………………………… Date: ……………………..

Hunton
Church of England
Primary School

Staff Acceptable Use Policy 2020-21

As a professional organisation with responsibility for children's safeguarding it is important that all 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 Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

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

- 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**.**

- 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.

- 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.

- 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.

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

- 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. This may include data being 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 agreement and will always reflect parental consent.

- 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 network to upload any work documents and files in a password protected environment or via VPN.

- 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.

- I will respect copyright and intellectual property rights.

- 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 for my school.

- 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 ICT Technician team as soon as possible.

- 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 Designated Safeguarding Lead /or Headteacher.

- 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 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 and the Law.

- 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.

- 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.

- I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. I will report any concerns immediately to a senior leader and IT technician.

- I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

- 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 Designated Safeguarding Lead and/or Headteacher.

- 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.

- 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

Twitter and Social Media

- I have read and am aware of our Twitter Policy and risk assessment.

- I am aware I am an ambassador for the setting. I will be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

- I will always act within the legal frameworks within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.

- I will ensure appropriate consent has been given before sharing images on the official social media channel. I will not disclose information, make commitments or engage in activities on behalf of the setting, unless I am authorised to do so.

- I will not engage with any private/direct messaging with current or past learners or parents/carers.

- I will inform my line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……………………….... Print Name: …………………….. Date: ……………………..

Wi-Fi Acceptable Use Policy 2020-21

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.

The school provides Wi-Fi for the school community and allows access for (school / education use only*).*

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.

The use of ICT devices falls under Hunton CEP School school's Acceptable Use Policy, online safety policy, behaviour policy and safeguarding/child protection which all pupils/staff/visitors and volunteers must agree to and comply with.

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.

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.

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.

The school's wireless service is not secure, and 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.

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.

The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

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.

I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

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.

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.

I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the Headteacher.

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 Hunton CEP School Wi-Fi Acceptable Use Policy.

Signed: ………………………... Print Name: ……………………… Date: ………

Hunton
Church of England
Primary School

PTA Social Networking Acceptable Use Policy 2020-21

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

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 (using Facebook, Twitter, WhatsApp) is a public and global communication tool and any content posted may reflect on the school, its reputation and services.

I will not use the site/page/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.

I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead or 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 the site 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.

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.

I will follow the school's policy regarding confidentiality and data protection/use of images.

- I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
- Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on the site will not be forwarded to any other person or organisation.

I will promote online safety in the use of the site and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account.

- The school Designated Safeguarding Lead or the Headteacher will have full admin rights to the account.

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.

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

I will ensure that the site is moderated on a regular basis as agreed with the Designated Safeguarding Lead or the Headteacher.

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.

If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead or the Headteacher.

I have read, understood and agree to comply with Hunton CEP School PTA Social Networking Acceptable Use Policy

Signed: ………………………... Print Name: ……………………… Date: ………

Accepted by: …………………………… Print Name: ………………………….

Hunton
Church of England
Primary School

Official Social Networking Acceptable Use Policy for Staff 2020-21

For staff running official school social media accounts

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 the school website, Twitter, are public and global communication toosl and that any content posted may reflect on the school, its reputation and services.

I will not use the sites 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.

I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead or the Headteacher. The Headteacher retains the right to remove or approve content posted on behalf of the school.

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.

I will follow the school's policy regarding confidentiality and data protection/use of images.

- This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
- Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on the sites will not be forwarded to any other person or organisation.

I will promote online safety in the use of Twitter / school website 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.

I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used.

- The school Designated Safeguarding Lead and/or Headteacher will have full admin rights to the sites.

Where it believes unauthorised and/or inappropriate use of the sites 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.

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.

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

I will ensure that the site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

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.

If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead or the Headteacher.

I have read, understood and agree to comply with the Hunton CEP School Social Networking Acceptable Use policy.

Signed: ………………………... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………

Hunton
Church of England
Primary School

Consent Form - Use of Images of Children 2020

Generally photographs are a source of pleasure and pride. We believe that the taking and use of photographs can enhance the self-esteem of children and their families and therefore is something to be welcomed and appreciated.

We may take photographs for a number of reasons whilst your child is with us, including:
Displays around school
For the school prospectus and school website
Documenting and recording education activities
Recording their learning and development progress
Recording special events and achievements

We will also encourage children to be active learners, and to become involved in using cameras themselves by taking photos of their surroundings, activities and of each other.

We do however recognise that with the increase in use of technologies, particularly digitally and online, the potential for misuse has become greater and we understand that this can give rise to concern. We will therefore endeavour to put effective safeguards in place to protect children and young people by minimising risk.

We are mindful of the fact that some families may have reasons why protecting a child's identity is a matter of particular anxiety. If you have special circumstances either now or at any time in the future which would affect your position regarding consent, please let us know immediately in writing.

We include the safe use of images as part of our Online Safety Policy, which you can view on the school website. We include photos of pupils on our school website and Twitter / Instagram account if we have the correct permissions to do so. On occasions the school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

To comply with current GDPR requirements and the Data Protection Act, we require your permission for the following. Please could you answer the questions below, then sign and date the form where shown.

Childs Name……………………………………Class …………………… Please circle your answer

1. May we use your child's photograph (with no name) in publications that we may produce for promotional purpose including the school prospectus, website and Twitter. Yes / No

2. May we use your child's photograph (with first name) in publications that we may produce for promotional purpose including the school prospectus, website and Twitter. Yes / No

3. May we use video footage of your child (with no name) in publications that we may produce for promotional purposes including the school prospectus, website and Twitter. Yes / No

4. May we use video footage of your child (with first name) in publications that we may produce for promotional purposes including the school prospectus, website and Twitter. Yes / No

5. Do you consent to your child's photograph being published by the press or media (as described above - In this event the school will do their best to ensure that only the child's first name is published) Yes / No

Conditions of use of images by the school

1. This form is valid from the date you sign it, for the period your child attends school. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your agreement at any time.

2. The school will not use the personal details or full names (first name and surname) of any child in a photographic image on video, school displays or in any other of our printed publications.

3. If we use photographs or video of individual pupils, we will not use the surname of that child in the accompanying text or photo caption, unless we have your agreement.

4. We may use group or class photographs or video footage with has very general labels, such as “a science lesson” or “fun at the fete”

5. We will only use images of pupils who are appropriately dressed, to reduce the risk of images being used inappropriately.

6. As the child’s parent/carer we agree that if we take photographs or video recordings of our child/children which include other pupils, we will use these for personal and family use only. I/we understand that where consent has been obtained from other parents for any other use, we would be in breach of Data Protection Act 1998 if we used our images for any wider purpose. We will not post images of other children (i.e. not our own children) on the internet e.g. social networking sites without the express permission of their parent/carer.

7. The school will take photos and video footage to celebrate learning for use in school without permissions from parents / carers. These will be stored securely on the school network if digital and possibly printed for use on display or in photo albums.

- I have read and understood the conditions of use and I am also aware of the following:
    - Websites and social media sites can be viewed worldwide; not just in the United Kingdom where UK law applies.
    - The press are exempt from GDPR and Data Protection Act and may want to include the names and personal details of children and adults in the media.
- I/we will discuss the use of images with our child/ren to obtain their views, if appropriate.
- As the child’s parents/guardians, we/I agree that if we/I take photographs or video recordings of our child/ren which include other children, then we will only use these for our personal use.

……………………………………………… ……………………………
Signature of Parent / Carer Date