Preston Candover CE Primary School

Love, Hope and Justice

Online Safety, Mobile Technology and Acceptable Use Policy

November 2019	**Review Date:** March 2021
	Signed by Headteacher:
	Reviewed by: IT Leader

Contents

Procedures

1. Introduction

This policy applies to all members of the school community (including staff, pupils, governors, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety, Mobile Technology and Acceptable Use Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our school's vision for Online Safety

At Preston Candover CE Primary School, we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our Online Safety, Mobile Technology and Acceptable use policy.

Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view Online Safety education as a key life skill.

Our Online Safety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. Online Safety Roles in School

Our Online Safety Leader is the Computing/IT leader
Our Website is administered by the Admin team
Our DSLs are Mrs Simrit Otway and Mrs Cathy Taylor

The role of the Online Safety Leader/ Computing/IT Leader

- Ensuring that policy is implemented and that compliance with the policy is actively monitored.
- To be aware of procedures to be followed in the event of a serious online-safety incident.
- Ensure the school uses an approved filtered internet service, which complies with current statutory requirements.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools' IT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the SLT, staff, pupils and governors are updated on as necessary.
- Takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents (including Acceptable Use Policies).
- Liaising closely with the school's Designated Senior Person/Child Protection Officer / nominated governor to ensure a co-ordinated approach across relevant safeguarding areas.
- Promotes an awareness and commitment to e-safeguarding throughout the school community.
- Ensures Online Safety education is embedded across the curriculum.
- To facilitate training and advice for all staff.

The role of the Network Manager / Agile / Hampshire IT

- To ensure the integrity and security of the school network and Firewall
- To supply regular maintenance of all hardware in school (Agile).

The role of the teachers:

- To embed Online Safety issues in all aspects of the curriculum and other school activities.
- To supervise and guide pupils carefully when engaged in learning activities involving online technology and mobile technology.
- To ensure pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

To deliver online the safety element of computing curriculum.

The role of all staff:

- To read, understand and help promote the school's online-safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
- To be aware of online-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- To report any suspected misuse or problem to the Online Safety leaders

- To maintain an awareness of current online-safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

The role of the Pupil:

- Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good online-safety practice when using digital technologies out of school and realise that the school's Online-safety Policy covers their actions out of school, if related to their membership of the school

The role of Parents / Carers:

- To understand the school's policy regarding the importance of adopting good online-safety practice when using digital technologies out of school and reinforce this in the home
- To ensure they and their child have read and signed the Acceptable Use Policy for the relevant Key Stage.

4. Policies and practices

This Online Safety, Mobile Technology and Acceptable Use Policy should be read in conjunction with the following other related policies and documents:

- **Acceptable Use Policies**
- **Safeguarding /Child Protection Policies**
- **LA Guidance On The Use of Social Networking Sites And Other Forms Of Social Media**
- **Behaviour and Positive Relationships Policy**

4.1 Security and data management

Computing/IT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Hampshire Computing/IT Security Framework should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of General Data Protection Regulation, sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

1. Accurate
2. Kept safe and secure
3. Used fairly and lawfully
4. Used for limited, specifically stated purposes
5. Handled in accordance with the data subject's rights
6. Adequate, relevant and not excessive
7. Kept no longer than absolutely necessary
8. Only transferred to others with adequate protection
9. All laptops are password protected

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

• School 's equipment, including laptops, must only be used for school purposes and do not contain personal information e.g., personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times.

Any breaches in security must be reported immediately to the Data Protection Officer (DPO).

• School equipment must not be used for non-educational purpose, for example for online gambling, dating websites, home shopping, booking holidays, social networking BOTH at home and in school.

• Staff are aware of the school's procedures for disposing of sensitive data, e.g., shredding hard copies, deleting digital information, deleting usernames and passwords from school's system when children leave, deleting email accounts, IEPs, SATs information and know the person responsible should there be any queries.

• The school's policy is to remove sensitive data prior to disposal or repair of equipment and all staff are aware of the person responsible.

• Remote access is available to SLT

• School data shall NOT be stored on personal equipment, e.g, home computer or mobile phone.

• Staff are allowed to use personal storage devices, e.g, external hard drives, pen drives in school to transfer data from home but this must be kept secure with encryption, passwords and virus checkers ran on device before usage.

• Staff must ensure they log out of computers when out of use and all computers will go to the screen saver screen after 10 minutes only allowing access to those with a password. No confidential information is stored on individual computers so to limit its accessibility.

4.2 Use of mobile devices

• In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, all mobile devices can only access the school's broadband internet connection if set up by the school technician with permission of the Headteacher/Admin Officer.

This includes school based laptops and teacher laptops and does not include personal phones, netbooks and other internet enabled devices unless specified.

Ipads are now in use at school and these do not currently have security software available, however any online resources still need to pass through the schools strict filtering system. Apps are put on ipads via Computing/IT leader/Agile only.

4.3 Use of digital media (cameras and recording devices) In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

Pupil Images/Photos/Videos

On admission, all parents/carers will be asked to sign the consent for photos to be taken in school or by the media for use in relation to promoting/publishing the school e.g. school prospectus/school website/school displays.

This consent will last for a maximum of 7 + 1 years only. The consent will be gained when the child starts school at Preston Candover CE Primary School (Reception class).

This does not cover any other agency and if any other agency requests to take photographs of any child then separate consent before photographs are taken will be sought. Images will not be displayed if parents do not agree.

Our policy is to only use images where groups of children are involved in activity that represent the work that pupils are doing thus enabling the school to celebrate our achievements to others.

We allow parents/carers to take photos of special events/ school activities when invited but to not focus on any child but their own.

In order to support this policy, we would ask parents/carers not to use any images of our pupils on social networking sites (i.e. Facebook). This includes any professional photos that have been purchased through the school and any photos taken during school concerts or sports events etc. It is acknowledged that often photographs may contain other children in the background.

Staff can photograph and record events on school equipment.

Staff images/photos/videos

Images of staff are not displayed on our websites etc. to ensure they are not misused. Images of staff at work are not allowed to be used on social media and can only be used in media/the school website if permission is given for each individual photo/image. This will be removed if staff leave their position.

Photos of staff taken outside of school are not affected by this but it should be considered as to whether images on social media will bring into disrepute your integrity, as well as the potential misuse of these images.

Storage of Photographs / Video

Under General Data Protection Regulation, the school must seek parental consent to take photographs and use video recorders. Parents will be asked to sign a pupil 'Using images & video Multimedia Consent form' at the beginning of the academic year.

All staff log on with their username and passwords.

Photographs are displayed in school; on the website; in the school prospectus as well as in the media. Photographs for school use and taken for school purposes must only be taken with school equipment and remain on school premises.

These images/videos must only be stored on school equipment in school. Pupils must be appropriately dressed for the activity they are partaking in considering health and safety and hygiene.

The school will monitor the use of equipment and storage of images. Any problems with security and storage will be logged and dealt with via training and disciplinary.

- Photographs are securely stored and should not be removed from the school environment unless for a specific purpose and with the head teacher's consent. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets.
- Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used
- Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices.
- Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted.
- Access to photographs / videos stored on school's equipment is restricted to school staff.
- Should a parent withdraw permission the class teacher is responsible for the removal and deletion of images and may be assisted by the Computing/IT subject leader.
- Photographs sent electronically must be sent securely. This is done using staff accounts on the HCC e-mail system.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email:

- All digital communications should be professional in tone and content via an HCC email address only.
- Email is considered a secure way of transferring data from home to school and is encouraged via a secure HCC email address.

- Staff have access to their own work email account and this will be used in correspondence with all work related activities/communications. These will be accessed via a username and password only. Personal email addresses will not be used.

Email is covered by the GDPR and freedom of information act and safe practise will be followed in using email to ensure confidentiality. School email addresses may be monitored at any time in accordance with the acceptable use policy.

- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- Social networking sites (i.e. Facebook) are becoming increasingly popular amongst the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. **Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and anyone providing false information is violating the site 'Statements of rights'**.

For this reason, we would actively discourage pupils in our school using any social networking sites where these restrictions apply. Pupils who are found to be misusing websites where derogatory comments against other pupils, members of staff or the school are being made will have their internet access rights in school removed and in serious cases further action will be taken. Staff must also consider the security settings of these sites and if it will compromise their position in school. If this occurs staff may be disciplined or in extreme cases, outside agencies may become involved.

Mobile Phones, Cameras and wearable technologies

Staff personal mobile phones:

- The school does not permit the use of personal mobile phones and cameras by staff and visitors where children are present
- Staff and visitors will not carry personal mobile phones while working. This protects staff from being distracted from their work, and from allegations of inappropriate use. Staff phones will be kept either in the staffroom or in their bags in a secure cupboard.
- If staff have a break time during their working hours, they may use their mobile phones during these times, in the staffroom or office away from the children.
- Where it is essential for staff to make a personal call during a session, they should (with the agreement of SLT) make this in an area not used by children.

- Staff must give the school telephone number to their next of kin, in case it is necessary for the staff member to be contacted, in an emergency during session hours.
- Mobile phones will be taken on whole-group outings in accordance with guidance. This will be used only to communicate with other teachers, school, emergency professional, or parents when appropriate and in an emergency. Mobile phones will not be used to take photos during these outings. School camera or iPads will be used following the online safety policy requirements.
- In the case of school productions and events, parents are requested to only take photos of their child/ren and not to post on social media sites.
- In EYFS – no assessment photos can be taken by staff on their mobile phones, these must be taken on a school ipad as per school policy.

Children

• No child is allowed a mobile device in school. If a child brings a mobile device in for a special circumstance or by 'mistake' the phone will be locked away for the duration of the day and handed over to the parents at home time.

• The school displays a notice advising visitors and parents/carers that mobile phones are not to be used in the setting. If they need to use their mobile phone they will be asked to use this away from the children. Visitors will be asked to switch their phones onto silent while in school

• No videos, photos are allowed at social events such as plays/ performances/ sports day unless invited to do so on an individual child basis.

• Individual 1 on 1 photos can be taken as long as no other child is present and it is the child of the designated parent or guardian

• All parents/ guardians are requested not to put these images on social networking sites

Emergencies

If a child needs to contact his/her parents/carers they will be allowed to use the school phone. If parents need to contact their children urgently they should phone school office and leave a message and this message will be relayed to the child and/or child's teacher.

Responsibilities for mobile phones

School accepts no responsibility theft, loss or damage relating to mobile phones. It is the responsibility of staff and parents to ensure that mobile phones are properly insured

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

We do not encourage or use instant messaging other than when secure messaging is taught and used as part of a lesson. If an inappropriate message is sent then this is followed up and children or disciplined, parents contacted and outside agencies if appropriate are contacted.

Web sites and other online

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- The school website is maintained by the school office and the website provider, e4education with relevant event information and newsletters. It is also an access point to some of our school policies including this Online safety and AUP. Only the head and office can access and amend the school website and all ensure no personal data is displayed online.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing (SKYPE, WebEx etc)

- Approval by the Headteacher shall be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Others:

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. We will update our policy to reflect what we consider to be acceptable and unacceptable use of these as and when required and this is an ongoing process.

4.5 Acceptable Use Policy (AUP)

Our Acceptable Use Policy (AUP) is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of Computing/IT for educational, personal and recreational purposes.

We have AUPs for staff, pupils and visitors and they are signed and adhered to by users before access to technology is allowed. A list of pupils who, for whatever reason, are not allowed to access technology is kept in school and made available to staff.

- **In our school the following statements reflect our practice in the use of our AUP's.**
  - They are understood by the individual user and relevant to their setting and purpose.
  - They are reviewed regularly and updated with the support of school governors.
  - They are regularly communicated to all users, particularly when changes are made to the Online Safety Policy/AUP.
  - They outline acceptable and unacceptable behaviour when using technologies, for example:
    Cyberbullying
    Inappropriate use of email, communication technologies and Social Networking sites and any online content
    Acceptable behaviour when using school equipment/accessing the school network.
  - They outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
  - They provide advice for users on how to report any failings in technical safeguards.
  - They clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
  - They outline sanctions for unacceptable use and make sure all users are aware of the sanctions.
  - They stress the importance of Online Safety education and its practical implementation.
  - They highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.6 Dealing with incidents

Our school will consider the types of incidents that may occur and how these will be dealt with. An incident log will be completed to record and monitor offences. This is kept with the Online Safety, Mobile Technology and Acceptable Use Policy in the Headteacher's office. These will be audited on a regular basis by the Headteacher and reviewed by the Governing Body H & S Committee. All staff are aware of the different types of Online Safety incident (illegal and inappropriate) and how to respond appropriately. Pupils are informed of these procedures via assemblies, in class and through reading and signing the AUP. The Headteacher will decide at which point parents or external agencies are involved. The school uses the Online Safety Incident/Escalation Procedures document (see Appendix 4) as a framework for responding to incidents.

Illegal Offenses

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who will refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF). We will **never personally investigate, interfere with or share evidence as this may cause us to inadvertently commit an illegal offence.** We will always report illegal content to the IWF as they are licensed to investigate – we are not!

Correct procedures will be followed when preserving evidence to protect those investigating the incident and are as follows:

- Turn off the monitor (Do NOT turn off the system)
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff)

• Make a note of the date/time of the incident along with any relevant summary details
• Contact our school's neighbourhood policing team for further advice

Examples of illegal offences are:

• Accessing child sexual abuse images
• Accessing non-photographic child sexual abuse images
• Accessing criminally obscene adult content
• Incitement to racial hatred

Inappropriate Use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and are proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

INCIDENT	PROCEDURE AND SANCTIONS
ACCIDENTAL ACCESS TO INAPPROPRIATE MATERIALS	•Minimise the webpage/turn the monitor off • Tell a trusted adult • Enter the details in the Incident Log and report to filtering services if necessary • Persistent 'accidental' offenders may need further disciplinary action
USING OTHER PEOPLE'S LOGINS AND PASSWORDS MALICIOUSLY	•Inform Headteacher • Enter details in the Incident Log • Additional awareness raising of Online Safety issues and the AUP with individual child/class • More serious or persistent offenses may result in further disciplinary action in line with Behaviour Policy • Consider parent/carer involvement
DELIBERATELY SEARCHING FOR INAPPROPRIATE MATERIALS	
BRINGING INAPPROPRIATE ELECTRONIC FILES FROM HOME	
USING CHATS AND FORUMS IN AN INAPPROPRIATE WAY	

5. Infrastructure and technology

Pupil Access:
They will work with an adult or under the supervision of an adult on the computers and must report all problems and not attempt to solve them alone.

Passwords:
A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Staff and children have a separate password. The staff password is changed regularly to ensure integrity. Admin passwords are known only to Computing/IT coordinator and technician. All school members are reminded of the importance of passwords and their security. If compromised these are changed instantly.

Software/hardware:
All software is licensed and up to date and licences are kept by the school.

Managing the network and technical support:
Agile IT and the IT Leader update and repair school computers and laptops. Laptops without staff support.

Filtering and virus protection:
Filtering is controlled by HCC. This is high level security but is not impenetrable and if incidents occur, the incident flowchart procedures must be followed. The school uses ESET endpoint protection and security software as recommended by HCC on all computers and laptops.

6. Education and Training:

We recognise that education and training are essential components of effective Online Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online Safety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote Online Safety. Online Safety messages are communicated to the various stakeholder groups in our school community via Online Safety Rules posted in all rooms where computers are used and discussed with pupils regularly. Online Safety is embedded within the Computing/IT scheme of work, in our assemblies and throughout the curriculum. There are three main areas of Online Safety risk that our school is aware of and considers:

Area of Risk	Examples of Risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. virus', Trojans, Spyware Premium rate services, Online gambling

Content Pupils need to be taught that not all content is appropriate or from a reliable source	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cybertattoo, sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies	Grooming Cyberbullying Contact inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

6.1 Online Safety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own Online Safety. Preston Candover CE Primary provides suitable Online Safety education to all pupils:

- We provide regular, planned Online Safety teaching within a range of curriculum areas. We also have an additional focus on Online Safety during the National Online Safety Awareness Week/ Safer Internet Day.
- Online Safety will be differentiated for pupils with special educational needs.
- Pupils are made aware of the relevant legislation when using the internet and of the impact of cyber bullying and how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- We ensure that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of Computing/IT both within and outside school.
- Pupils are reminded of safe internet use through classroom displays, Online Safety rules (see Appendices) and acceptance of AUP

Cyber bullying (using technology to bully others) is dealt with using the same methods as described in the Behaviour and Positive Relationships Policy, taking into account the PSHE policy and taking into account all discrimination policies. In the case of unsuitable or illegal content or usage, the flowchart (see appendices) is followed.

6.2 Online Safety – Raising staff awareness

- All Staff are regularly updated on their responsibilities as outlined in our school Online Safety, Mobile Technology and Acceptable Use policy.
- This training is provided as and when required by our Headteacher and DSL

- The Online Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Networking Sites.
- All staff are expected to promote and model responsible use of Computing/IT and digital resources.

- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff/team meetings.

6.3 Online Safety – Raising parents'/carers' awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it" (Byron Report, 2008)

- Our school offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies. For example through:
- School newsletters, website and other publications.
- We provide Online Safety awareness sessions and promote external Online Safety resources/online materials.

6.4 Online Safety – Raising Governors' awareness

The school ensures that Governors, particularly those with specific responsibilities for Online Safety, Computing/IT or child protection, are kept up to date with Online Safety issues through discussions at governor meetings and attendance at Local Authority Training.
The Online Safety Policy will be reviewed regularly (and/or if a serious breach occurs) by the IT Leader, approved by the governing body and made available on the school's website.

7 Standards and inspection

The implementation of our policy will be monitored, recorded and reviewed on a regular basis by our IT Leader – Headteacher, SLT, staff and governors.
Online Safety incidents will be monitored and analysed to see if there is a recurring pattern such as specific days, times, classes, groups and individual pupils.
Any patterns will be addressed by working with a specific group, class assemblies or reminders for parents.
This monitoring will contribute to any changes in the policy and practice.
Staff, parents/carers and governors are informed of changes to policy and practice by newsletter, assemblies, staff and governor meetings, letters and on our school website. AUPs are reviewed on a regular basis and include *reference to current trends and new technologies.*

8 – Online Safety Incident Log

All Online Safety incidents must be recorded by the School or designated person. This incident log will be monitored and reviewed regularly by the Headteacher/DSLs. Any incidents involving Cyberbullying should also be recorded on the 'Integrated Bullying and Racist Log'

Appendix 1 Using images & Video
Multimedia consent form

To **Name of the child's parent or guardian:** _____

Name of child: _____

Occasionally, we may take photographs or produce videos for school purposes that include our pupils. We may use these images in our marketing or in other printed publications that we produce, as well as on our website, on our social media or on project display boards. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

From time to time, our 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 the General Data Protection Regulation of 2018, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer questions 1 to 5 below, then turn over and sign and date the form where shown.

The information you provide (address, contact numbers) will be securely stored and processed within the European Economic Area (EEA) and not be used for any other purpose than confirming your permission to use the material.

Please return the completed form to the school as soon as possible.

	Please circle your answer
1. May we use your child's photograph in printed publications that we produce for promotional purposes or on project display boards?	**Yes / No**
2. May we use your child's image or video on our website?	**Yes / No**
3. May we record your child's image on video or webcam?	**Yes / No**
4. Are you happy for your child to appear in the media	**Yes / No**
School to delete this question where social media not used. 5. Are you happy for your child to appear on Social Media sites used by the school e.g. Twitter and Facebook - *Please note that once images are uploaded, they will be subject to the terms and conditions of the social media site. Neither you nor the school will have control over how those images are further used, amended or reproduced, either by the site or by the public. Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK European law applies.*	**Yes / No**

Conditions of use

1. This form is valid for seven years from the date you sign it, or for the period of time your child attends this school, plus one year. The consent will automatically expire after this time.

2. We will not re-use any photographs or recordings after your child leaves this school.

3. We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.

4. If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See point 3 above.)

5. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

6. We may include pictures of pupils and teachers that have been drawn by the pupils.

7. We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'making Christmas decorations'.

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

9. Your consent can be withdrawn at any time in writing.

10. Images and videos will only be stored within the EEA in order to conform to the GDPR of 2018.

11. If we wish to retain any images or video for the school's historical archives, we will seek written permission from a child's parents with full and transparent reasons to support the request.

12. After a cohort leaves the school we will archive students' work for a period of one year. This will securely be stored and hidden from open view on the school network. Parents of students can request evidence of a child's work for up to one year after that child's cohort has left the school by submitting a Subject Access Request (SAR) via the school office. After the archive year has passed students data will be completely removed from the school network and become unrecoverable.

Please note that the press have some exemptions from data protection legislation and may want to include the names and personal details of children and adults in the media.
I have read and understood the conditions of use and give my consent for my child's image/s & videos to be used as described above.

Your signature ……..…….. Date ……
Your name (in block capitals) …….

Appendix 2

Preston Candover CE Primary School

Love, Hope and Justice

Model Policy on Staff Acceptable Use of ICT

1.0 Introduction

1.1 This model policy has been developed on behalf of all Hampshire maintained schools. Whilst Governing Bodies are advised to develop their own policy through consultation with staff and staff representatives to reflect their own systems and arrangements in school, it is appreciated that maintained schools that use Hampshire ICT services will have broadly similar requirements and therefore could adopt this policy for their own use.

1.2 Schools that do not use Hampshire ICT Services are likely to need to adjust this policy to reflect the systems in place in their school.

1.3 This Policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- School Social Media Policy
- Information Security – Corporate Acceptable Use Policy
- E-mail, Internet and Intranet Monitoring Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedure

1.4 Schools are encouraged to ensure that staff are given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Schools and their staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com). Advice can also be sought from professional associations and trade unions.

2.0 Application

2.1 This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

2.2 The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any

other electronic or communication equipment used in the course of the employee or volunteer's work.

2.2 This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

3.0 Access

3.1 School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

3.3 Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), SIMS, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

3.5 Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

3.6 If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

3.7 No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

3.8 Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

3.9 The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4.0 Communication with parents, pupils and governors

4.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

4.1.2 Text System – All Teachers and Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

4.1.3 Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Headteacher before sending. Where office staff send letters home these will normally require approval by the Headteacher/Administrative Officer.

4.1.4 Email – school email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.1.5 Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school's policy on home visits.

4.2 Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

5.0 Social Media

5.1 School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that

inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

5.2 Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6.0 Unacceptable Use

6.1 Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

6.1.1 to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;

6.1.2 to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;

6.1.3 to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;

6.1.4 to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;

6.1.5 to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils;

6.1.6 to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

6.1.7 to collect or store personal information about others without direct reference to The Data Protection Act;

6.1.8 To use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

6.1.9 to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school;

6.1.10 to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people;

6.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources

including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

6.3 Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

6.4 Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

7.0 Personal and private use

7.1 All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

7.1.1 taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

7.1.2 interfering with the individual's work

7.1.3 relating to a personal business interest

7.1.4 involving the use of news groups, chat lines or similar social networking services

7.1.5 at a cost to the school

7.1.6 detrimental to the education or welfare of pupils at the school

7.2 Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

7.3 It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

7.4 Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable

staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

7.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

8.2 Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

8.3 School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

8.4 Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.

8.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

8.6 Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

8.7 The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

8.8 Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

8.9 Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

9.0 Monitoring

9.1 The school uses Hampshire County Council's ICT services and therefore is required to comply with their email, internet and intranet policies.

9.2 The school and county council reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

9.2.1 to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised

9.2.2 to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems

9.2.3 to gain access to communications where necessary where a user is absent from work

9.3 Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

9.4 To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

10.2 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

10.3 Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

11.0 Signature

11.1 It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

11.2 Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

Do's and Don'ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school's ICT resources and facilities
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.

- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……..….

NAME (PRINT): ……

Appendix 3

Preston Candover CE Primary School
ICT Acceptable Use
Pupil Agreement/Online Safety Rules

It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the internet.

- I will only use ICT in school for school purposes
- I will only use the internet and/or online tools when a trusted adult is present
- I will not deliberately look for, save or send anything that could be unpleasant or nasty
- I will not deliberately look for, or access inappropriate websites
- I will not bring into school any electronic mobile devices e.g. cameras, phones, smart watches etc.
- I agree to use the school iPad camera and microphone functions in a sensible way and under supervision
- If I accidentally find anything inappropriate I will tell my teacher immediately
- I will only communicate online with people that a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not give out my own, or others', details such as names, phone numbers or home addresses
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will not attempt to download or install anything onto the school network without permission
- I will be responsible for my behaviour when using ICT because I know these rules help to keep me safe
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety

<u>Pupil's agreement:</u>
I have read and understand the school rules for responsible internet use and technology.

Pupil's signature: …… Date: …….

<u>Parent/carer signature:</u>
I have read and understand the school rules for responsible internet use and technology. We have discussed this and …… (print child's name) agrees to follow the online safety rules and to support the safe use of ICT at Preston Candover CE Primary School.

Parent/carer name (PRINT): ……

Parent/carer name (signature): …… Date: ……

Appendix 4

Incident Log

Date / Time of Incident	Type of Incident	Name of pupil/s and staff involved	Incident details	Resulting actions taken and by whom (and signed)

APPENDIX 5 – Responding to Online Safety Incident/ Escalation Procedures