Copthorne Preparatory School

Online Safety Policy 2025-26

Information Technology Department

Policy Author:	Mark Bone (Head of Digital & Innovation / DDSL)
Created:	01-08-2025 (Version 2.0)
Approved by SLT:	
Ratified by the Governing Body:	
Date of Next Review:	01-09-2026

Review Date: 01-08-25	Version: 2.0	Reviewed by: M Bone
Reference to KCSIE updated to 2025 Headmaster updated to Head of School		
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:
Review Date:	Version:	Reviewed by:

This is a whole School policy and applies to all members of Copthorne Preparatory School including EYFS

Introduction

In today's society, members of the Copthorne Preparatory School community interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes, and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all but can occasionally place members of our community in danger.

Online safety covers issues relating to the safe use of the Internet, mobile phones, and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with our pupils.

As a school, we must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating pupils and staff about responsible use. We must be aware that pupils and staff cannot be completely prevented from being exposed to risks both on and offline. Pupils should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the pupils in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. This is achieved through regular in-service training sessions.

Breaches of online safety policies can and have led to civil, disciplinary, and criminal action being taken against staff, pupils, and members of a wider school community in establishments across the country. It is crucial that all members of the Copthorne Preparatory School community are aware of the offline consequences that online actions can have. This online safety policy is essential in setting out how we at Copthorne Preparatory School plan to develop and establish our online safety approach and to identify core principles which all members of the school community need to be aware of and understand.

This policy should not be used to address issues where other policies and procedures exist to deal with them. It is intended to both supplement and complement any such documents and should be read in conjunction with the following:

- Safeguarding Policy
- Keeping Children Safe in Education 2025
- Wellbeing Policy
- Behaviour Policy
- Anti-bullying Policy
- EDI Policy
- Searching a Pupil Policy
- Staff/Volunteer - IT Acceptable Use Policy (Appendix A)
- Pupil IT Acceptable Use Policy (Prep School) (Appendix B)
- Parent IT Acceptable Use Policy (Prep School) (Appendix C)
- Pupil IT Acceptable Use Policy (Pre-Prep School) (Appendix D)
- Pupil IT Acceptable Use Policy (EYFS) (Appendix E)
- Social Media Policy (Appendix F)
- Filtering Policy (Appendix G)
- Online Safety Rules (Appendix H)
- Mobile Phone Policy (Appendix I)
- Remote Working Guidelines (Appendix J)
- Taking, Storing and Using Images of Pupils Policy (Appendix K)
- Use of Digital Images / Video Agreement (Appendix L)
- AI Policy (Appendix M)

- Parental Consent for RileyBot (Appendix N)
- Pupil iPad Acceptable Use Policy (Appendix O)
- Online Safety Incident Report Form (Appendix P)

The breadth of issues classified within online safety is considerable and ever evolving but can be categorised into four areas of risk - content, contact, conduct and commerce.

Pupils increasingly use electronic equipment on a daily basis to access the internet, share and view content and images via social media sites and interact online. Many children now have unlimited and unrestricted access to the internet via mobile networks - 3G, 4G and now 5G, which some of them may abuse to harass their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content. Online access can also be misused to send hurtful or abusive texts or emails, and to groom and entice children to engage in extremist, criminal or sexual behaviour such as webcam interaction or face-to-face meetings.

Pupils may also be distressed or harmed by accessing inappropriate material such as pornographic websites or those which promote extremist behaviour, criminal activity, suicide or eating disorders.

All pupils are taught about online safety throughout the curriculum and all staff receive online safety training which is regularly updated. In line with the requirements of KCSIE 2025, the DSL has lead responsibility for online safety, supported by a DDSL with specialist knowledge of online safety, monitoring and filtering. In addition, the designated Safeguarding Governor, also has responsibility for online safety.

The School will follow the guidance around harmful online challenges and online hoaxes when supporting children and sharing information with parents/carers.

Pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL will consider a referral into the Cyber Choices programme. This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

This 'Online Safety Policy' forms part of the safeguarding policies, as well as being the overarching document supporting the suite of IT policies. It is compiled by the Head of IT and DSLs and reviewed regularly in line with regulatory change and developing technological trends.

Teaching and learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As well as affording excellent research opportunities, it also enables the sharing and review of work through our Apple TV mirroring system, flipped learning opportunities, innovative ways of submitting and of marking work, as well as disseminating notes and information. Beyond this, and perhaps more importantly, the routine use of iPads and technology prepares pupils for a world which is increasingly dependent on digital technologies.

Pupils are taught what internet use is acceptable and what is not and are given clear objectives for internet use; they are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. They are shown how to publish and present information appropriately to a wider audience and are taught how to evaluate internet content and how to validate information before accepting its accuracy. Above all the school endeavours to ensure that pupils are critically aware of the materials they read. The school always seeks to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Managing Information Systems

It is important to review the security of the whole school IT System from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g., the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site must be encrypted.
- Portable media must not be used without an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Network Manager/Head of IT will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in other countries and in different continents can be created, for example.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries. Whilst restriction of incoming and outgoing email to approved addresses is possible and the filtering for unsuitable content is in use, the system is not fool proof and as such, pupil education in the safe use of email is vitally important.

In the school context (as in the business world), email should not be considered private, and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils, and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils should only use their school email accounts for school purposes. Personal email accounts should not be used to communicate with members of staff or to submit work.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone.
- Staff should only use their official school provided email accounts to communicate with pupils and parents/carers. Where parents/carers are relatives or personal friends of members of staff, a clear distinction should be maintained between their professional and social interaction. The school provided email account should be used for all professional correspondence and a personal email account for any social correspondence.

- Access in school to external personal email accounts may be blocked for some/all user groups for part or all of the day as deemed appropriate by SLT.
- Email sent to external organisations should be written carefully and where necessary, authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

Published Content

We, in line with many schools, have created an excellent website through which it is possible to inspire pupils to publish work of a high standard. Our website can celebrate pupils' work, promote the school, and publicise its achievements.

Publication of any information online should always be considered from a personal and school security viewpoint. Some information may be better published on the Parent Portal which requires authentication.

- The contact details on the website should be the school address, email, and telephone number. Staff or pupils' personal information must not be published.
- Email addresses should be published carefully online, to avoid being harvested for spam (e.g., by replacing '@' with 'AT'.)
- The Head of Marketing has overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing Pupils' Images and work

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' full names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's consent. Full details regarding the use of digital images can be found in our policy on taking, using, and storing images of children (Appendix K).

Pupils also need to be taught the reasons for caution in publishing personal information and images online. This should form part of the work covered with them on online safety

- Images or videos that include pupils must be selected carefully and must not provide material that could be reused.
- Pupils' full names must not be used anywhere on the website, particularly in association with photographs.
- Confirmation of consent from parents or carers must be checked before images/videos of pupils are electronically published (Appendix L).
- Consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The school will maintain a policy regarding the use of photographic images of children which outlines policies and procedures (Appendix K).

Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes, and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers, and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. The school's policy on social media (Appendix F) should be adhered to at all times. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, etc.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests, and clubs etc.

Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

- Staff official blogs or wikis should be password protected and run from the school website or vle with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding pupils' use of social networking, social media, and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the schools Social Media Policy (Appendix F).

Filtering and Monitoring

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community.

Staff may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, where legitimate use can be confirmed, it is possible for restrictions to be removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent, or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.

It is important that pupils, staff, and parents recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g., mobile phone). Occasionally mistakes may happen, and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that our Acceptable Use Policies are adhered to. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online.

Incidents involving breaches of filtering or inappropriate content being accessed will be fully investigated by the Safeguarding Team if found to not be part of a legitimate lesson eg. Sex Education in Science, Drug Awareness in PSHE, Online Safety in IT lessons. Procedures are in place to report such incidents to parents once the matter has been fully investigated. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, Surrey Police or CEOP.

Staff should always evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering and monitoring appropriate to the age and maturity of the pupils or the staff member's role within the school.
- The Head of IT and SLT will ensure that the filtering policy (Appendix G) is continually reviewed.
- All breaches of filtering must be reported to the DSL and Head of IT immediately. Full details including the names of those involved, time, date and if possible suspect URL should be included. There should be no parental contact until the matter has been fully investigated.
- If staff or pupils discover unsuitable sites, the URL must be reported to the DSL and Head of IT who will then record the incident and escalate the concern as appropriate.
- Requests for changes to the school filtering eg. allowing a particular website, will only be actioned once it has been approved by the DSL in line with the requirements of KCSIE 2024
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Surrey Police or CEOP.

Child Produced Sexual Imagery

Youth produced sexual imagery, problematic or harmful sexual behaviour and child on child abuse can all happen online. If staff are concerned that an incident of this nature has taken place, they should refer to the detailed guidance in the School's Safeguarding Policy and contact the DSL who will follow guidance set out in KCSIE 2025 and in the UK Council for Internet Safety's 'Sharing nudes and semi-nudes' which can be found here. Under no circumstances should images be viewed.

Creating or sharing explicit images of anyone under 18 is illegal. The school will respond swiftly to ensure pupils are safeguarded, supported and educated.

Managing Videoconferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

Schools may also decide to use conferencing services such as Skype, Zoom and Teams. Meetings / lessons should always be booked as private and not made public. The meeting URL should only be given to those who you wish to take part.

- All videoconferencing equipment must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information must not be put on the school website.
- Pupils must ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- When recording a videoconference lesson, written permission should be given by all participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for your class.

Managing Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration, and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch. The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype, and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication but is often not possible.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or smart watch with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance, text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework.

There are dangers for staff however if personal phones are used to contact pupils and therefore a school owned phone should be issued.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy (Appendix I).

Protecting Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The General Data Protection Regulations gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under these regulations, every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The General Data Protection Regulations applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The regulations set out standards which must be satisfied when processing personal data (information that will identify a living individual). The regulations also give rights to the people the information is about i.e., subject access rights let individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Policy Decisions

Authorising Internet Access

Copthorne Preparatory School will allocate Internet access to staff and pupils on the basis of educational need. Via the user lists held by the Network Manager, it will be clear who has internet access and who has not. Authorisation is generally on an individual basis in the Prep School. In the Pre-Prep and Nursery, where pupil usage should be fully supervised, pupils are often authorised as a group rather than an individual.

Normally, most pupils will be granted Internet access, although Parental permission is sought before agreement is given (Appendix C/D/E). Staff must be aware that pupils should not be prevented from accessing the internet unless the parents have specifically denied permission, or the pupil is subject to a sanction as part of the school behaviour policy.

- The school will maintain a current record of all staff and pupils who are granted access to the school's IT systems.
- All staff will read and sign the Staff / Volunteer Acceptable Use Policy (Appendix A) before using any school IT resources.

- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the school's network will be asked to read and sign an Acceptable Use Policy (Appendix A)
- Parents will be informed that pupils will be provided with filtered Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type

- EYFS access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- Pre-Prep pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Prep pupils will apply for Internet access individually by agreeing to comply with the school's online safety rules and the pupil Acceptable Use Policy.

Assessing Risk

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the fact that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

- Copthorne Preparatory School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- Copthorne Preparatory School will audit IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act and breaches may be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to Incidents of Concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. An e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others.

e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the schools Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the Senior Leadership Team should determine the level of response necessary for the

offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The DSL/DDSL/e-Safety Coordinator will record all reported incidents and actions taken in MyConcern or 'CHIP' and in any other relevant areas e.g. Bullying or Safeguarding log.
- The Designated Safeguarding Lead will be informed of any online safety incidents involving safeguarding concerns, which will then be escalated appropriately.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will escalate the concern to the Police.

Handling Online Safety Incidents

Teachers and pupils should know how to report an online safety incident (Appendix P). The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online safety incidents may have an impact on pupils, staff, and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious, and a range of sanctions may then be required, linked to the school's disciplinary policy. Potential safeguarding or illegal issues must be referred to the Designated Safeguarding Lead. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Police.

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse will be referred to the Head od School and DSL.
- All online safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaint's procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and safeguarding procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress, or offence to any other members of the school community.

Managing Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming, or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents
- gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, they should seek assistance from the police.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded and investigated.
- Pupils, staff, and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff, and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Managing Virtual Learning Environments

An effective virtual learning environment can offer schools a wide range of benefits to teachers, pupils, and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- The Virtual Learning Environment (vle) must be used subject to careful monitoring by the Head of IT/Network Manager. As usage grows throughout the school then more issues could arise regarding content, inappropriate use and behaviour online by users.
- IT staff/DSL will regularly monitor the use of the vle by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the vle.
- Only members of the current pupil, parent/carers and staff community will have access to the vle.

- All users will be mindful of copyright issues and will only upload appropriate content onto the vle.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

Any concerns about content on the vle may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the vle for the user may be suspended.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

Managing Mobile Phones and Other Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA , MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render pupils or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode.
- Mobile phones with integrated cameras could lead to Safeguarding, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

A policy which prohibits pupils from taking mobile phones to school could be considered to be unrealistic for schools to achieve. Many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a phone. However, the nature of our school environment and the fact that all children are transported to and from school, most often by their parents, means that the current policy of not allowing pupils to have mobile telephones in school is not unreasonable.

However, due to the widespread use of personal devices it is essential that Copthorne Preparatory School take steps to ensure, on the occasions that they are allowed, that mobile phones and devices are used responsibly. Staff should also be given clear boundaries on professional use.

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the school Mobile Telephone Policy (Appendix G).
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices should not be used during lessons or formal school time.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft, or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets, and swimming pools.

Pupils Use of Personal Devices

- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the school in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Communication

Introducing the Online Safety Policy to Pupils

As pupils' perceptions of the risks will vary; the online safety rules will need to be explained or discussed. Copies of our online safety rules should ideally be displayed in every room with a computer to remind pupils of the online safety rules at the point of use.

Consideration must be given as to the curriculum place for teaching online safety. Whilst the major role is taken by the IT Department as part of their online safety awareness programme, there is also a role to play by the teachers of every subject, whenever pupils are using the internet.

- All users will be informed that network and Internet use will be monitored.
- An online safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An online safety module will be included in the IT curriculum covering both safe school and home use.
- Online safety training will be part of the transition programme when moving between sections of the school.
- Online safety rules or copies of the Pupil Acceptable Use Policy will ideally be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to online safety education will be given where pupils are considered to be vulnerable.

Introducing the Online Safety Policy to Staff

It is important that all staff feel confident to use new technologies in teaching and the school's e–Safety policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse are specific and that instances resulting in disciplinary procedures and dismissal have occurred in many other schools. If a member of staff is concerned about any aspect of their IT or internet use either on or off site, they should discuss this with the Head of IT or the Senior Leadership Team to avoid any possible misunderstanding.

Particular consideration is given when members of staff are provided with devices by the school which may be accessed outside of the school network. Specific policies are clear regarding the safe and appropriate use of the school equipment and rules exist regarding use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

Induction of new staff should include a discussion about the school e–Safety Policy.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor IT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Enlisting Parents' Support

Internet use in pupils' homes is increasing rapidly, encouraged by low-cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents to understand more about IT, perhaps by running courses and parent awareness sessions (although the resource implications will need to be considered).

- Parents' attention will be drawn to the school e–Safety Policy in newsletters and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an Acceptable Use Policy Agreement.

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Appendix A

Staff/Volunteer IT Acceptable Use Policy - Whole School

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

All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

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

IT Acceptable Use Policy Agreement

I understand that I must use the school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the Head of IT.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal

equipment to record these images, unless I have specific permission to do so. Where these images are published (eg on the school website / VLE) it should not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

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

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this IT Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.

Staff / Volunteer IT Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the IT Acceptable Use Agreement. If you do not complete and return this agreement, access will not be granted to school IT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school IT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg. mobile phones, tablets etc.
- I use my own equipment out of school in a way that is related to me being a member of this school eg. communicating with other members of the school, accessing school email, VLE, website etc.

Name:	
Signed:	
Date:	

Appendix B

Pupil IT Acceptable Use Policy - Prep School

New technologies have become integral to the lives of our pupils in today's society, both within school and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure:

- that pupils of Copthorne Preparatory School will be responsible users and stay safe while using the internet and other communication technologies for educational, personal, and recreational use.
- that Copthorne Preparatory School's IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Copthorne Preparatory School will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Copthorne Preparatory School's IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the IT systems, email, and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school IT systems for on-line gambling, internet shopping, file sharing at any time or for on-line gaming, video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal handheld / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use age-appropriate chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement Form - Prep

Please complete the sections below to show that you have read, understood and agree to the rules included in this Acceptable Use Agreement. If you do not complete and return this agreement, access will not be granted to school IT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school IT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg. mobile phones, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school eg. communicating with other members of the school, accessing school email, virtual learning etc.

Pupil's Name:	
Form:	
Pupil's Signature:	
Date:	

Appendix C

Parent/Carer Acceptable Use Policy - Prep School

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Parents are requested to complete the permission form below to show their support of the school in this important aspect of the school's work.

Parent/Carer Acceptable Use Policy (Prep School) - Consent Form

As the parent / carer of the pupil named below, I give consent for my son / daughter to have access to the internet and to IT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Child's Name:	
Parent's Name:	
Parent's Signature:	
Date:	

Appendix D

Pupil IT Acceptable Use Policy - Pre-Prep School

New technologies have become integral to the lives of our pupils in today's society, both within school and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure:

- that pupils of Copthorne Preparatory School will be responsible users and stay safe while using the internet and other communication technologies for educational, personal, and recreational use.
- that Copthorne Preparatory School's IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Copthorne Preparatory School will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that my child must use Copthorne Preparatory School's IT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the IT systems and other users.

Internet access for Pre-Prep pupils is mainly limited to supervised use of approved websites.

You may feel that many of the rules included in our Acceptable Use Policy Agreement may not be relevant at this stage of your child's education although they may become so as they move further up the school.

At suitable age/developmental milestones, pupils will be expected to follow these rules:

For my own personal safety:

- I understand that the school will monitor my use of the IT systems, email, and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school IT systems for on-line gambling, internet shopping, file sharing at any time or on-line gaming or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my personal handheld / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use age-appropriate chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement Form - PrePrep

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not complete and return this agreement, access will not be granted to school IT systems for your child.

I have read and understand the above and agree that my child will follow these rules when:

- They use the school IT systems and equipment (both in and out of school)
- They use my own equipment in school (when allowed) eg. mobile phones, PDAs, cameras etc.
- They use my own equipment out of school in a way that is related to them being a member of this school eg. communicating with members of the school, accessing school email, virtual learning etc.

Childs Name:	
Class:	
Parents Name:	
Signed:	
Date:	

Appendix E

Pupil IT Acceptable Use Policy - EYFS

New technologies have become integral to the lives of our pupils in today's society, both within school and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure:

- that pupils of Copthorne Preparatory School will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that Copthorne Preparatory School's IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Copthorne Preparatory School will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

I understand that my child must use Copthorne Preparatory School's IT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the IT systems and other users.

Internet access for EYFS pupils is mainly limited to supervised use of approved educational websites.

At suitable age/developmental milestones, pupils will be encouraged to follow these rules:

- I will take care when using the school IT equipment and use it properly.
- When asked, I will share using the computer with other pupils.
- I will tell an adult if I see anything that upsets me.
- I will be aware of stranger danger.
- I will only take photographs or video of someone if they say it is alright.
- I will not write anything which upsets other people.
- I understand that the school may talk to my Parents/Carer if they are worried about my use of school IT equipment.
- I understand that if I do not follow these rules, I may not be allowed to use the school computers or internet even if it was done outside of school.

Pupil Acceptable Use Agreement Form - EYFS

Please complete the sections below to show that you have read, understood, and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, then your child will not be granted access to school IT systems.

I have read and understand the above and agree to encourage my child to follow these rules when:

- they use the school IT systems and equipment (both in and out of school)
- they use my own equipment in school (when allowed) eg. mobile phones, cameras etc.
- they use my own equipment out of school in a way that is related to them being a member of this school eg. communicating with members of the school, accessing school email, virtual learning etc.

Pupils Name:	
Class:	
Parents Name:	
Signed:	
Date:	

Appendix F

Staff Social Media Policy

Introduction

Copthorne Preparatory School is fully aware and acknowledges that increasing numbers of adults and children are making use of social networking sites.

The widespread availability and use of social networking brings opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance aims to protect and inform staff and to help and advise Senior Leadership on how to deal with potentially inappropriate use of social networking sites.

Purpose

The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

Objectives

The policy aims to:

- Assist staff to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal, or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Head of School of the justification for any such action already taken or proposed.

This policy should not be used to address issues where other policies and procedures exist to deal with them. It does not replace or take priority over advice given by Children's Services, the school's codes of conduct dealing with allegations of abuse, other policies issued around safeguarding children or IT issues (email, IT and data protection policies), but is intended to both supplement and complement any such documents.

Scope

This policy applies to all adults who work at Copthorne Preparatory School. This includes teachers, support staff, supply staff, Governors, contractors, and volunteers. References to staff should be taken to apply to all the above groups of people. Reference to pupil's means all pupils registered at the school.

For the purpose of this policy, 'social networking sites' is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Sites such as Facebook, X, Instagram, Tik-Tok are perhaps the most well-known examples of social networking sites but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube. This definition of social networking is not exhaustive as technology develops with new ways of communicating advancing every day.

All staff and pupils should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social networking sites in work time

The use of social networking applications for personal use is not permitted during normal work time. Where the filter timings allows, staff should ensure that any use during their breaks and non-contact periods does not interfere with any legitimate work related use of the IT Systems by other members of staff.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head of School first.
Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head of School. However, staff must still operate in line with the requirements set out within the policy

School Social Media Accounts

Establishing New School Social Media Accounts

There are numerous social media accounts including school, departmental and community accounts, across all platforms, with most regularly posting online. Updated guidance and best practise is shared with staff running these accounts regularly and support is always available at any time from the Marketing Department. If you are setting up a school or school community channel and are a member of staff or an official volunteer, you must contact the Marketing Department before starting. They can help you make best use of your presence and ensure you adhere to brand guidelines and messaging. Before establishing a new account, staff should consider whether their audiences and objectives cannot be met through an existing account. Official School accounts must not be established or run by pupils. The school retains the right to refuse the setting up of new school or school community channels.

Management of Accounts

All School social media accounts must adhere to the school's brand guidelines and give clear indication of their purpose. If several members of staff run the same social media account, a designated account manager should be agreed and have a system in place to regularly monitor, update and manage the content of any official School account and ensure questions posted are responded to promptly. If negative comments are posted by viewers, please contact the Marketing Department immediately for support.

Posting from School Accounts

All social media posts from Copthorne Preparatory School accounts represent the institution. It is important that every post is carefully considered, appropriate and designed to enhance the reputation of the school. If possible, measures should be put in place to avoid communication errors, including checking of content by a third party.
Anyone posting on school accounts will be viewed externally as representing the institution. All content posted or otherwise promoted must be courteous and respectful of others inside the school and in the wider community. Staff should remember the power imbalance they hold with pupils and should be wary of negative interactions which may be interpreted in a way different to that intended.
Care should always be taken to ensure the content is properly considered and not in breach of the civil or criminal law before it is posted. Social media content must not:

- discuss the inner workings of the school or reveal future plans or ideas that have not yet been made public.
- contain private or confidential information regarding an individual, company or organisation or about the school itself.
- reveal details of intellectual property belonging to the school.
- breach any confidentiality rules pertaining to the school.
- identify a pupil other than using their first name and use or share pupils' images without checking permission is given.

The school reserves the right to remove content on School and school community channels.

Account Security

Account hacking represents a significant risk to social media accounts and can lead to the spread of harmful misinformation and extensive reputational damage for the host organisation and individual community members.
Every School and school community account must have an agreed manager with responsibility for choosing strong, secure passwords. Passwords should be securely stored, not in files on shared drives or on paper. The current passwords for all School and School community accounts must be sent to the Marketing Department. In cases of emergency, such as hacking, the school's Senior Leadership Team may need urgent out of hours access to any School or school community social media account.
It is good practice to regularly renew passwords. Staff should also secure accounts with 2- factor authentication. If more than one member of staff has access to the account, the account manager is responsible for collating and maintaining a log of staff with access to the account's password and the password must be changed whenever one of those staff members moves on to a different role or different institution.

Concerns and Issues

If a school account has been hacked, or a post is attracting negative comments and it is not clear how to respond, staff should flag with the Marketing Department and seek advice.
Social media activity on staff or pupils' accounts that raises welfare concerns should be reported in line with the School's Safeguarding policy. Social media activity on pupils' or staff accounts which constitutes misconduct should also be reported in line with the School's Staff Code of Conduct Policy.

Terms of Use

Staff must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all staff. This includes, but is not limited to, public facing applications such as open discussion forums and internally facing uses such as project blogs regardless of whether they are hosted on the school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Copthorne Preparatory School expects that users of social

networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual, or offensive nature that may bring the school into disrepute.
- Must not be used in an abusive or hateful manner.
- Must not be used for actions that would put staff in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies.
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with. Caution should also be taken before becoming 'friends' with ex-pupils who are over the age of 18 where siblings continue to attend the school.
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head of School.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.
- Staff need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, could result in formal action being taken against them.

Violation of this policy can/may be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/protection for staff on using social networking

General

- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Due care should be taken where family and friends have pupils in school.
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils and staff interacting using social networking sites, please contact the Designated Safeguarding Lead in school

Personal Responsibility

- Copthorne Preparatory School staff are personally responsible for the content they publish online. Staff should be mindful that what they publish will be public for a long time. Once materials have been published online, they may be out of the control of the publisher.

- Online behaviour should reflect the same standards of honesty, respect, and consideration that is used face-to-face and should be carried out consistent with the standards applied on school premises and in furtherance of the School's Mission.
- When posting to a blog, discussion forum, X or Facebook account, staff must ensure that they make it clear that the information is representative of their views and opinions and not necessarily the views and opinions of Copthorne Preparatory School. Blogs, wikis, discussion groups, and podcasts can be seen as an extension of the classroom. What is inappropriate in the classroom should be deemed inappropriate online.
- The lines between public and private, personal and professional are blurred in the online world. By virtue of identifying themselves online as affiliated with Copthorne Preparatory School, staff are now connected to colleagues, pupils, parents and the school community. Staff should therefore ensure that content associated with them is consistent with their work at the school.
- Staff should not participate in spreading false or unsubstantiated rumours or false information.
- Staff should strive to speak the truth - and when they don't know, sometimes saying nothing is the best choice.
- When contributing online staff must not post confidential pupil information.
- Before posting videos and photographs of pupils to any online forum, including Facebook, a blog or any other media, prior permission in writing of the Parents/Carer must be obtained.
- Such materials should ONLY be posted to social media that provides reasonable protection against general public access and has tools in place to limit access only to identified or invited persons.

Disclaimers

- Copthorne Preparatory School staff must include disclaimers within their personal blogs and other media in which they either identify themselves or are likely to be identified as affiliated with the school that the views are their own and do not reflect on Copthorne Preparatory School. For example, "The postings on this site are my own and do not necessarily represent the positions, strategies, or opinions of Copthorne Preparatory School."
- Where online media is open to content and participation (such as comments) from pupils and parents, teachers are encouraged to carefully review and moderate such comments or disable their use.

Guidance/protection for Pupils on Using Social Networking

General

- No pupil may access social networking sites during the school working day.
- Mobile phones are not permitted in school unless permission has been given for a particular purpose such as a school trip.
- No pupil should attempt to join a staff member's areas on networking sites.
- No school computers are to be used to access social networking sites at any time of day unless such access forms part of the legitimate school curriculum.
- Any attempts to breach firewalls will result in a ban from using school IT equipment other than with close supervision
- Please report any improper contact or cyber bullying to your Form Tutor, DSL, Matron etc. as soon as it happens.
- We have a zero tolerance to cyber bullying

Personal Responsibility

- Be aware of what you post online. Social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.
- It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
- Be safe online. Never give out personal information and do not share your password.
- Do your own work! Do not use other people's intellectual property without their permission. Be aware that it is a violation of copyright law to copy and paste other's thoughts. It is good practice to hyperlink to your sources.
- Be aware that pictures, videos, songs, and audio clips may also be protected under copyright laws. Verify you have permission to use the images, videos, songs or other clips.
- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
- Blog and wiki posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.
- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.

Protection of Personal Information

Adults working in schools should:

- Never share their work logins or passwords with other people.
- Keep their personal phone numbers private
- Not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used. Where parents are also friends, a clear distinction should be maintained between professional and social interactions.
- Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.
- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Adults working in schools should not:

- Use school equipment for personal use, e.g. cameras
- Use their own mobile phones to contact pupils or parents.

Communication between pupils / adults working in school

Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, webcams, websites and blogs.
The school normally provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for a particular trip. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.
Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

Adults should not give their personal contact details to pupils including home e-mail addresses, home, or mobile telephone numbers, unless the need to do so is agreed with senior leadership and parents/carers. E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites.

Child safeguarding guidance

If the Head of School receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above, they should:

- Record the disclosure in line with the safeguarding policy
- The school must refer the matter, also in line with the safeguarding policy.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
- If disclosure comes from a member of staff, try to maintain confidentiality
- The Governors and Head of School, in consultation with the necessary Authorities, will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been taken.
- If disclosure is from a child, follow the normal process in the safeguarding policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no pupil use of social networking sites on school premises, Copthorne Preparatory School protects themselves from accusations of complicity in any cyber bullying through the provision of access.
Parents should be clearly aware of the school's policy of access to social networking sites.
Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

This can be a complex area, and these examples might help:

- A child is receiving taunts on Facebook and text from an ex-pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends using Facebook and Instagram. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: This is the tricky one. The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school but refuse to deal with the social networking issues.

Once disclosure is made, investigation will have to involve the families. This should be dealt with under the schools adopted anti bullying policy.

If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment
This guidance can also apply to text and mobile phone cyber bullying.

Appendix G

Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the DSL and Head of IT. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
To ensure that there is a system of checks and balances and to protect those responsible, any changes to the school filtering service must be logged.

All users have a responsibility to report immediately to the DSL or Head of IT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through online safety awareness sessions.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Head of IT who will decide in consultation with the DSL what action is required.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use agreement.

Appendix H

Online Safety Rules (for display in all classrooms)

These online safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- I understand that the school owns the computer network and the iPad I have been given and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- I will only use IT systems in school, including the internet, email, digital video, iPad, etc., for school purposes. I will not use IT systems at school for private purposes, unless the Head of School has given specific permission.
- I will not use IT systems at school for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will only log on to the school network, Wi-Fi or learning platforms (such as Teams) with my own username and password.
- I accept that I am responsible for all activity carried out under my username.
- I will follow the school's IT security guidelines and not reveal my passwords to anyone
- I will only use my school email address for school-related work
- I will make sure that all IT communications with pupils, teachers or others is responsible and sensible, particularly as emails could be forwarded to unintended readers.
- I will not send anonymous messages or chain mail.
- I will be responsible for my behaviour when using any online or digital services. This includes resources I access and the language I use.
- I will be polite and appreciate that other users might have different views to my own.
- I will contribute to discussion spaces positively and will share my ideas constructively.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using any of the online services I have signed up to.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher and with the full knowledge and approval of my parents/carer.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher. I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will not download or install software on school technologies.
- I will not attempt to bypass the internet filtering system.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I understand the school can exercise its right to monitor the use of the school's computer systems and learning platform, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I understand that all my use of the internet, school's learning platform and other related technologies can therefore be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted. I understand that irresponsible use may result in the loss of my internet access or iPad.

Appendix I

Mobile Phone / Smartwatch Policy

Introduction

Copthorne Preparatory School recognises that personal communication through mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately and safely.

The widespread ownership of mobile phones and smart watches has led to the requirement that as a school we take steps to ensure that they are used responsibly by all members of the Copthorne Preparatory School community. This Policy is designed to ensure that potential issues involving mobile phones and smart watches can be clearly identified and addressed, ensuring that the benefits that mobile phones and smart watches provide can continue to be enjoyed.

All members of the Copthorne Preparatory School community must read, understand, and abide by the policy as a condition upon which permission is given to bring mobile phones to school.

The policy for mobile phones and smart watches also applies during school excursions, residential trips, and extra-curricular activities both on the school campus and off-site.

Responsibility

It is the responsibility of the person who brings the mobile phone or smart watch to school to abide by the guidelines outlined in this document.

When specific permission has been granted allowing for pupils to bring a mobile phone to school, the decision to provide a mobile phone to their children should be made by parents or carers. It is incumbent upon parents to understand the capabilities of the phone and the potential misuse of those capabilities. Pupils are not permitted to wear smart watches in school.

Parents/carers should be aware if their child takes a mobile phone to school, it is assumed household insurance will provide the required cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.

Parents/carers are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any relevant way. Passing messages through school reception also reduces the likelihood of disrupting lessons inadvertently.

Pupil Use of Mobile Telephones

Many parents/carers may give their children mobile phones to protect them from everyday risks involving personal security and safety. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently. However, our situation remains somewhat different to that experienced by most schools as pupils do not travel to school by themselves. As such, the current rule is that pupils may not bring mobile phones into school unless they have been given specific instructions to do so for an outing or special event. The exceptions to this rule are for weekly boarders who may bring a mobile phone into school with them although it must be handed to the Boarding Housemaster for safe keeping and may only be used at his discretion and for pupils travelling to

school using public transport who should hand their phone in to the school office on arrival and collect it from there on their departure.

Where specific permission has been granted, pupils must adhere to the following:

- Mobile phones and personally owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft, or damage of mobile phones.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, swimming pool and toilets.
- The Bluetooth functionality of a mobile phone should be switched off at all times and may not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones without the prior consent of the person or people concerned.
- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences and encouraged to use PIN's and other security as necessary.
- Pupils should also understand that the school also has the right to take action against them if they are involved in incidents of inappropriate behaviour, that are covered in this policy, when out of school and where they involve their membership of the school community (examples would be cyber-bullying, use of images or personal information).

Staff Use of Mobile Telephones and Smart Watches

The school recognises the importance of emerging technologies present in modern mobile phones e.g., camera and video recording, internet access, etc. Whilst teachers may wish to utilise these functions to aid teaching and learning it is the safety and well-being of the Copthorne Preparatory School community, themselves included, that must take priority.

In line with published guidelines, mobile telephones, cellular enabled smart watches and personal devices with photographic capability must not be used in the EYFS setting and should be secured away in the lockers provided.

- Staff should never contact pupils from their personal mobile phone or give their mobile phone number to pupils.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for example a mobile on school trips or staff-based landline in departments or school offices. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school

owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

- Mobile phones and personally owned devices must be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices must not be used during teaching periods and other work periods, meetings etc. (including for the sending of text, emails and the use of the internet functionality) unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Approval by a member of the senior leadership team must be explicitly given before staff and/or children may use mobile phones or a personal device as part of an educational activity. Generally, there will need to be a good educational reason for the activity to take place.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils. School equipment will be provided for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to breaks, lunch break and other non-work periods.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, the online safety coordinator or DSL should be contacted.

Acceptable Uses

Parents/carers are requested that in cases of emergency they contact the school first. This ensures that staff are aware of any potential issue and may make the necessary arrangements.
Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the school.
Pupils should protect their phone numbers by giving them only to close friends and family. This will help protect the pupil's number from falling into the wrong hands and guard against insulting, threatening or unpleasant communications.
If asked to do so, pupils will show the content requested or hand their phone to a teacher or other designated adult such as the police.

Theft or damage

The responsibility of keeping a mobile phone safe lies with the person who has brought it onto the school premises; the school accepts no responsibility for replacing lost, stolen, or damaged mobile phones. When a mobile phone is found on the school premises and the owner cannot be located, it should be handed into the school office.

It is strongly advised that passwords and/or pin numbers are used to ensure that unauthorised phone calls cannot be made (e.g., by pupils, or if stolen). Lost and stolen mobile phones in the U.K. can be blocked across all networks making them virtually worthless to the thief.

Inappropriate conduct

Using mobile phones to bully or threaten pupils or staff is unacceptable. Cyberbullying will not be tolerated. In some cases, it could constitute criminal behaviour. Using technology to humiliate, embarrass or cause offence will not be tolerated; regardless of whether 'consent' was given.

It is forbidden for pupils to use their own or other pupil's mobile phones to take videos and pictures of acts to denigrate or humiliate others. This also includes using mobile phones to photograph or film any pupil or member of staff without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

Mobile phones are not to be used or taken into changing rooms, swimming pool or toilets or used in any situation that may cause embarrassment or discomfort to their fellow pupils, staff, or visitors to the school.

It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the pupil will be asked and expected to delete those images.

Any pupil who uses vulgar, derogatory, or obscene language while using a mobile phone will face disciplinary action.

Pupils may not engage in personal attacks, harass another person, or post private information using SMS messaging, taking/sending photos or objectionable images, and phone calls. Pupils using mobile phones to bully other pupils will face disciplinary action. [It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the police.]

Pupils must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence.

Sanctions

Pupils who infringe the rules set out in this document could face having their phones confiscated by teachers. If the phone is being used inappropriately the pupil must give it to a teacher if requested.

On any infringement of this policy the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. The pupil's parents or carer will be able to collect the mobile phone at the end of the school day and a record will be made of the incident.

If the incident involves pupils under the age of 13 or is deemed illegal or inappropriate, then staff have a duty to inform the DSL who may refer the incident to the police.

Appendix J

Remote Working Guidelines

Introduction

Remote access and working digitally from home are a normal and accepted part of working at Copthorne Preparatory School. There are a number of ways in which staff access and create content for work purposes and these guidelines aim to give clear parameters as to how data should be accessed and processed when not on site. All users should be aware of their own responsibilities when accessing data remotely and working off site; these responsibilities are primarily around confidentiality and data protection.

Definitions

Remote Access: accessing Copthorne Preparatory School systems from outside of Copthorne Preparatory School using any internet-enabled device. The information accessed and processed continues to reside on Copthorne Preparatory School systems, whether these be on site or in the cloud.
Mobile Working: carrying out work (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of Copthorne Preparatory School from outside of Copthorne Preparatory School premises.

User responsibilities and good working practices

The primary responsibilities of employees of Copthorne Preparatory School and other users that remote into the Copthorne Preparatory School network are to:

- Know what information they are accessing, using or transferring
- Understand and adhere to contractual, ethical or other requirements attached to the information and in line with Copthorne Preparatory School policies and procedures.
- Users are responsible for following correct procedures when logging out of the remote session (in particular RDS and OneDrive)

Responsibilities for data/ information accessed and/ or processed during mobile working

- Confidential data/information should not be created, stored or processed on privately owned computers, however this is permissible if you are saving directly to OneDrive and do not store copies of the data/information elsewhere
- 3rd party devices should not be considered or assumed to be secure and the use of such devices for storing documents or other work related to Copthorne Preparatory School is discouraged.
- Appropriate precautions and good practice should be followed for all data and information that has been edited, created and/or saved on mobile or home devices or other forms of media

Security of privately owned internet-enabled devices

If users are using their own personal systems or other mobile devices to carry out work for Copthorne Preparatory School using web-based applications such as OneDrive and iSams then the following points should be followed:

- Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner
- Maintain safe web-surfing practice.

- Each device should be kept up to date with anti-virus software
- Maintain good practice with use and storage of passwords
- Do not respond to unsolicited emails or click any link within unsolicited emails, popups and other means of communication that are not relevant to their role.
- Mobile devices should not be left unattended
- Ensure data that is deemed confidential is not left visible on screens in public areas
- If a system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at Copthorne Preparatory School, this is reported as soon as possible to the Network Manager / Head of IT.

Security of Copthorne Preparatory School devices

The use of a school-provided iPad or other device provided by the school is considered secure for remote access as long as the following additional guidelines have been enacted:

- Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner
- The iPad has a passcode and the 'lock screen automatically' function is enabled
- Return the device to IT Support if you encounter any system faults or any other security related issues
- Maintain safe web-surfing practice.
- Avoid saving any work locally on the iPad – use OneDrive wherever possible for any work
- Passwords are kept private and not made available to other users
- iPads or other devices are not left unattended
- Data that is deemed confidential is not left visible on screens in public areas
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.
- School owned devices should not be used for personal IT requirements. As this could lead to downloading potential malware / unwanted files.
- These devices, should not be taken on holiday and devices should be secured whilst user is not using them.

Creating and processing data remotely

Data created remotely in connection to work should not be shared in any ways other than through Copthorne Preparatory School authorised platforms, namely: the school email system, CHIP and the 'share' feature built into office 365.

Users should carefully consider which platform to use when sharing content remotely. Sensitive data (that is not related to CHIP) should only be transmitted if necessary, and with password-protection enabled on the document. Passwords for these documents must not be sent in the same email as the documents

Remote Access for Third Party Suppliers

It is often necessary for third party suppliers to require remote access to install, upgrade or troubleshoot Copthorne Preparatory School systems.
These instances should be undertaken only by IT Support staff. If there is any requirement for virtual technical support, you will be required to bring the device into school so that this can be successfully and safely undertaken.

Removal of Remote Access Rights

Access rights for remote access may be changed or removed from any user at any time if there is deemed to be a breach of the conditions of use or the user's access is compromising the confidentiality, integrity and/or availability of Copthorne Preparatory School's systems or services.

The remote access rights of all employees and third-party users shall be removed upon termination of employment, contract, or agreement.

Appendix K

Taking, Storing and Using Images of Pupils Policy

Scope and aims of the policy

This policy seeks to ensure that images and videos taken within and by Copthorne Preparatory School are taken and held legally and that required thought is given to safeguarding all members of the community.

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

This policy must be read in conjunction with other relevant school policies including, but not limited to:

- Safeguarding Policy
- Data Protection Policy
- IT Acceptable Use Policies
- iPad Acceptable Use Policy

This policy applies to all images, including still and video content. All images will be used in a manner respectful of the Data Protection Principles. This means that images will be processed:

- fairly, lawfully and in a transparent manner
- for specified, explicit and legitimate purposes
- in a way that is adequate, relevant limited to what is necessary
- to ensure it is accurate and up to date
- for no longer than is necessary
- in a manner that ensures appropriate security
- The Data Protection Officer (DPO), supported by the DSL and senior leadership team are responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the school.

Parental consent

Written permission from parents or carers will be obtained before images and/or videos of children are taken, used, or published.

Written parental consent will always be sought to take and use photographs offsite for professional, marketing and training purposes.

Written consent from parents will be kept by Copthorne Preparatory School when children's images are used for publicity purposes, such as brochures or publications, until the image is no longer in use.

A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed, and the record will be updated accordingly.

Safety of images and videos

- All images taken and processed by or on behalf of Copthorne Preparatory School will take place using school provided equipment and devices.

- Staff will receive information regarding the safe and appropriate use of images as part of their data protection and safeguarding training.
- All members of staff, including volunteers, will ensure that all images are available for scrutiny and will be able to justify any images in their possession.
- The DPO and/or DSL reserve the right to view any images taken and can withdraw or modify a member of staffs' authorisation to take or make images at any time.
- Only official setting owned equipment and cameras will be used by staff to capture images of children for official purposes. Use of personal equipment and cameras by staff is prohibited.
- Any apps, websites or third-party companies used to share, host or access children's images will be risk assessed prior to use.
- Copthorne Preparatory School will ensure that images always are held in accordance with the General Data Protection Regulations (GDPR) and Data Protection Act, and suitable child protection requirements, if necessary, are in place.

Publication and sharing of images and videos

- Images or videos that include children will be selected carefully for use, for example only using images of children who are suitably dressed.
- Children's' full names will not be used on the website or other publication, for example newsletters, social media channels, in association with photographs or videos.
- Copthorne Preparatory School will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.

Use of Pupil Images for Identification and Security

- All pupils are photographed on entering the school and, thereafter at annual intervals for the purpose of internal identification. These photographs are held securely on our management information system as the pupil record also includes data such as name, address etc. Access to the MIS is limited and is role specific within the school.

Usage of apps/systems to share images with parents

- Copthorne Preparatory School uses Flickror similar apps to upload and share images of children with parents.
- The use of these systems has been appropriately risk assessed and the school has taken steps to ensure all data stored is held in accordance with GDPR and the Data Protection Act.
- Images uploaded will only be taken on school devices.
- All users are advised on safety measures to protect all members of the community e.g. using strong passwords, logging out of systems after use etc.
- Parents/carers will be informed of the expectations regarding safe and appropriate use (e.g. not sharing passwords or copying and sharing images) prior to being given access. Failure to comply with this may result in access being removed.
- Tapestry is used to record the children's development and progress in EYFS in order to inform parents. Only parents and staff have access to this system.

Safe Practice when taking images and videos

- Careful consideration is given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

- Copthorne Preparatory School will discuss the use of images with children and young people in an age-appropriate way.
- A child or young person's right not to be photographed is to be respected. Images will not be taken of any child or young person against their wishes.
- Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc

Use of Closed-Circuit Television (CCTV)

- All areas which are covered by CCTV will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.
- Recordings will be retained for a limited time only and for no longer than their intended purpose. All recordings are to be erased before disposal.
- Regular auditing of any stored images will be undertaken by the Data Controller and/or DSL or other member of staff as designated by the senior leadership team.
- If cameras record activities taking place on the premises which are of a criminal nature or give any cause for concern, then information will be referred to the appropriate agency.
- CCTV cameras will be appropriately placed within the setting.

Use of photos and videos of children by others

Use of photos and videos by parents/carers

- Parents/carers are permitted to take photographs or video footage of events for private use only.
- Parents/carers who are using photographic equipment must be mindful of others, including health and safety concerns, when making and taking images.
- The opportunity for parents/carers to take photographs and make videos can be reserved by Copthorne Preparatory School on health and safety grounds.
- Parents/carers are only permitted to take or make recording within designated areas. Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.
- The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.
- Parents may contact the DPO/DSL to discuss any concerns regarding the use of images.
- Photos and videos taken by Copthorne Preparatory School and shared with parents should not be shared elsewhere, for example posted onto social networking sites. To do so may breach intellectual property rights, data protection legislation and importantly may place members of the community at risk of harm.

Use of photos/videos by children

- Copthorne Preparatory School will discuss and agree age-appropriate acceptable use rules with children regarding the appropriate use of cameras, such as places children cannot take the camera, for example unsupervised areas, toilets etc.
- All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.
- Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.
- Photos taken by children for official use will only be taken with parental consent and will be processed in accordance with GDPR and the Data Protection Act.

- Parents/carers will be made aware that children will be taking photos/videos of other children and will be informed how these images will be managed. For example, they will be for internal use only and will not be shared online or via any website or social media tool.
- Photos taken by children for official use will be carefully controlled and will be checked carefully before sharing online or via digital screens.

Use of images of children by the media

- Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's, or other relevant media, requirements can be met.
- The identity of any press representative will be verified, and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.
- Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith.

Use of external photographers

- External photographers who are engaged to record any events will be prepared to work according to the terms of the settings online safety policy.
- Photographers will comply with GDPR and the Data Protection Act at all times.
- Images taken by external photographers will only be used for a specific purpose, subject to parental consent.
- Photographers will not have unsupervised access to children and young people

Appendix L

Use of Digital Images / Video Agreement – Whole School Form

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations during subsequent lessons. Images may also be used to celebrate success through their publication in the newsletter, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission via this agreement before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their full names.

Parents are requested to complete the permission form below to allow the school to take and use images of their children.

Permission Form

As the parent / carer of the pupil named below I agree / do not agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I also agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will seek permission from the parents/carers of those children before publishing the images for a wider audience eg. via social media sites, blogs etc.

Y - Agree
N - Do NOT agree

Pupils Name:	
Form:	
Parents Name:	
Signed:	
Date:	
Specific Allowances / Exclusions (If required)	

Appendix M

AI Policy

Scope

Copthorne Preparatory School is committed to providing an outstanding, innovative education within a safe and secure environment and the effective and appropriate use of technology is an important part of this. With iPads and internet access available to all, it is essential that we establish clear guidelines for the use of these resources. This policy aims to outline the acceptable use of AI-enabled software, including Chat GPT as an emerging technology which will form part of their educational experience.

Acceptable Use

All staff and pupils are expected to use technology responsibly and in accordance with the school's primary Acceptable Use Policies.

Use of AI-Enabled Software

The use of Chat GPT, Rileybot and other AI-enabled software is permitted within the school where the filtering allows, subject to the following guidelines:

- Pupils may not use AI-enabled software to impersonate others or engage in any activity that may be considered deceptive or malicious.
- Pupils may not use AI-enabled software to cheat or gain an unfair advantage in any academic task. Specifically, this means not submitting AI-created content without the necessary references or acknowledgments.
- Pupils must be aware that teachers may use AI-enabled software to assist with marking. They will be informed in advance of any instances where this will occur. Teachers will always review the accuracy and integrity of AI-enabled marking.
- Neither teachers or pupils should enter any personal, or identifiable data into any AI system without clear guidance or risk assessment in place.

Pupil Training

Whilst developments in AI-enabled technologies are constantly evolving, all pupils will be given clear guidelines and training in how to make best, effective and safe use of the programs they are likely to encounter and use most often. This training will be rolled out in a number of ways, via form tutors, class teachers and the Digital, EDGE & Wellbeing curricula.
Pupils will explore both the technical use and ethical implications of AI for their school work and wider personal and social use.

Ethics Statement

As a school, we are committed to ensuring that the use of technology is ethical and responsible. With reference to AI-enabled technology this includes:

- Data Privacy: Users must respect the privacy of others and avoid storing, sharing or use of any personal information without consent.
- Bias and Discrimination: Users must be aware of potential biases in AI-enabled software and avoid perpetuating discrimination or prejudice.
- Accountability: Users must take responsibility for their actions when using AI-enabled software, and report any concerns or issues to the appropriate people within the school.

Conclusion

The use of technology, including AI-enabled software, is an integral part of education in the 21st century. Our school is committed to promoting responsible and ethical use of these resources, and to providing a safe and secure environment for all staff and pupils. By following these guidelines, we can ensure that emerging technology is used in a way that benefits our community and promotes learning and growth.

Appendix N

Parental Consent for RileyBot

RileyBot is an AI chatbot designed specifically for young people, with learning and safety as its core principles. RileyBot is designed to behave like a learning assistant, working with the learner to find answers, rather than simply doing all of the work for the pupil. RileyBot has a number of safety features, including a teacher and parent dashboard. Both teacher and parent can login to their dashboard and see the conversations their pupil/child has had with RileyBot. Teachers are alerted in real time if the content of the conversation is deemed inappropriate, allowing them to take the necessary action. The application privacy policy can be viewed at:

https://sphinxai.education/wp-content/uploads/2024/01/PrivacyPolicy_website.pdf

Please complete this form to confirm whether you give consent for your child to use RileyBot:

Child's Name:	
Child's Year Group:	
Parent's Name:	
Parent's Signature:	I hereby give consent for my child to be given access to RileyBot
Date:	

Appendix O

Pupil iPad Acceptable Use Policy

Introduction

Copthorne Preparatory School is committed to using technology to further improve the learning experiences and achievements of all of our pupils. iPad technology provides the opportunity to inspire and motivate pupils to achieve their full potential and to engage them fully in their learning. We believe that the use of an iPad will enhance everyday learning and in particular will:

- Raise educational attainment
- Create a pupil centred curriculum which will provide engaging pupil centred lessons
- Enable pupils to access the most up to date educational resources
- Raise levels of engagement, motivation, and interaction
- Improve facilitation of different learning styles
- Promote remote learning
- Improve self-management

This policy applies to all pupils who have been issued with a school owned iPad on a 1to1 basis for use in school and at home. This policy is intended to compliment the school's wider Online Safety and IT Acceptable Use Polices. It is provided to make all users aware of their responsibilities associated with the use of Copthorne Preparatory School's technology resources. Failure to comply may result in these privileges being terminated and the appropriate disciplinary action may be taken.

Due to the changeable nature of Information Technology this policy will undergo periodic review and as such the school reserves the right to amend any sections or wording at any time.

General iPad Terms

iPad Ownership

As part of its commitment to use technology to further improve the learning experiences of its pupils, Copthorne Preparatory School has decided to issue your son/daughter with a school owned iPad for use during lessons at school and for remote learning when away from school. This device remains in the ownership of Copthorne Preparatory School and is not a gift.

Use of Copthorne Preparatory School's technology resources is a privilege, not a right. This privilege is not transferable to people not associated with the school and terminates when a pupil is no longer enrolled at Copthorne Preparatory School. At this time, the device together with its case, charger and cables must be returned to the school. Failure to comply will result in the cost of replacements being charged against your billing account. Overseas pupils may take their iPad out of the country when returning home during the holidays. However, failure to return the device will result in the full cost of a replacement being charged against your billing account.

During the time that the device is in your child's possession, Copthorne Preparatory School will have full supervision and in particular:

- The school retains ownership of all hardware.
- The school retains ownership of all apps.

- Copthorne Preparatory School will have full supervision of the device via the school's Mobile Device Management system. This will include the ability to install applications, software, documents, ebooks on to the device and turn on/off different features at selected times of the day.
- The school will provide all required components to ensure the iPad operates effectively in the classroom, including Wi-Fi access.
- The school maintains the right to filter internet content and manage the use and connection of the iPads to the school network.
- Any pupil who receives a school owned iPad must sign up and adhere to the terms stated in this Policy as well as the IT Acceptable Use Policy.

Taking Care of iPads

Pupils are responsible for the general care of the iPad in their possession. Any breakages, technical issues etc. must be reported to the school's IT Department at the earliest possible opportunity.
Pupils will be held responsible for ALL damage to their iPads where this damage has been caused deliberately or through neglect.

General Precautions

iPads should not be left unattended in any unsupervised area and where possible should be kept with a pupil at all times. iPads may be left in a school locker at break-time, lunchtime and during PE, Swimming and Games lessons. iPads should not be left in the changing areas of the changing rooms at any time or otherwise unsupervised in plain view.

Carrying iPads

The iPads supplied by the school are provided in an approved protective case. iPads must remain in these cases at all times. These cases should remain free of any writing, stickers or other graffiti other than those identification labels added by the IT Department.
The screens are particularly sensitive to damage from excessive pressure and/or rough treatment. Pupils should avoid placing too much pressure and/or weight (such as folders and workbooks) on the iPad screen.

Using iPads at School

iPads are intended for use at school each day. In addition to teacher expectations for iPad use, school messages, planners, calendars, and schedules may be available using the iPad. Therefore, pupils are responsible for bringing their iPad, fully charged, to all classes each day.
iPads should be taken home at the end of the school day for charging and should not be left in school overnight (unless by prior arrangement e.g. maintenance purposes).
Pupils should not lend or share their allocated iPad with other pupils unless expressly asked to do so by a teacher in a classroom situation.
If pupils leave their iPad at home, they are responsible for getting any assignments or coursework completed as if they had their iPad present. Spare iPads will not be available to pupils who forget to bring their iPad to school or who fail to charge their iPad.
Pupils who repeatedly (three or more times in a term) fail to bring the iPad to school/ or maintain a fully charged battery will be subject to further sanctions.
At all times, the class teacher's decision is final regarding use, or non-use of any iPad, collectively or individually.

Passcodes and Apple ID's

Pupils are expected to take reasonable measures to secure access to the iPad by using a passcode. Pupils are prohibited from removing the passcode from the device or sharing their passcode with anyone else except their parents or as requested by a designated member of the IT Department. Pupils must not attempt to access other pupil iPads by 'guessing' or trial and error passcode attempts.
School owned iPads are currently managed to prevent existing personal Apple ID's from being used. Apps are deployed to school owned iPads via Apple's Volume Purchasing Programme and the school's MDM software.

Digital Images/Video

Photographic images and video stored on the iPad must comply with the school's IT Acceptable Use Policy, Online Safety Policy and UK Law. The school reserves the right to randomly check any iPad for unsuitable content.
No images or video material taken in school may be uploaded from any device to social networking sites unless a pupil is asked to do so as part of a specific school project.
Recording, photographing, or filming within the classroom is only permitted with the permission of the class teacher. Permission must also be sought from anyone featuring in any recording, photograph, or video.

Sound, Music, Games

Sound must be muted at all times unless permission is obtained from the teacher for a specific task. Pupils may not listen to music via their iPads during lessons unless instructed to do so by the class teacher for specific educational purposes. Gaming on iPads is strictly prohibited at all times during the school day.

School Internet Access

Within school, pupils may only access the internet through "school-provided' wi-fi access. Pupils are not permitted to access the internet via a mobile connection or via proprietary hotspots as these provide unmonitored and unfiltered access. Copthorne Preparatory School is not responsible for any material accessed by a pupil in this manner.

Home Internet Access / iPad Use

Students are allowed to use their iPads at home for schoolwork and to set up wireless networks on their iPads to assist in this process. It is the responsibility of the Parent/Guardian to monitor and oversee iPad use within the home setting.
Parents/Guardians should be mindful of personal information stored by pupils on school provided iPads e.g. bank details/photographs. Copthorne Preparatory School will not accept responsibility for personal data that pupil's store. As a company we comply with the principles of the General Data Protection Regulation; we will process data lawfully and fairly and any data held will be kept secure and safe within our managed system.

Managing Your Files and Saving Your Work

It is the pupil's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. iPad malfunctions are not an acceptable excuse for not submitting work.
All pupils are provided with a Microsoft One Drive Account where work can be saved/backed up. This storage space may only be used for saving work directly related to Copthorne Preparatory School.

Software on iPads

Originally Installed Software

The school will provide software on iPads necessary for schoolwork. The Software/Apps originally installed by the school must remain on the iPad in usable condition and be easily accessible at all times. From time to time the school may add or modify software applications for use in a particular course.
The school's Mobile Device Management system monitors all apps that are installed on an iPad and will notify the IT Department of any changes that are made.

Inspection

Pupils may be selected at random, and without notice, to provide their iPad for inspection to check that they comply with this iPad Acceptable Use Policy as well as the school's IT Acceptable Use Policy.

Procedure for Reloading Software

If technical difficulties occur or illegal software is discovered, the iPad will be restored to the default factory settings. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

Software Updates

Upgrade versions of licensed Software/Apps are available from time to time. Students will be expected to download all updates prompted by Apple.

iPad / Student Identification

Student iPads will be labelled in the manner specified by the school. iPads can be identified in the following ways:
• Serial Number also known as the Mobile Device Management System ID
• A School Asset Management Label
Pupils should use their standard school IT username within apps not a nickname or other pseudonym.

iPad Security

Safety and Security

The school has invested in a Mobile Device Management system. This MDM system allows Copthorne Preparatory School to do simple things like send out apps and files automatically, to reset passcodes, update software and set restrictions to ensure iPads, when in school, work in accordance with the IT Acceptable Use policy. Limited restrictions can also be set for when the device is used away from school although it remains the responsibility of Parents/Guardians to oversee its use.
Pupils must never attempt to remove or circumnavigate this MDM system as importantly, it allows the school to protect the data on the iPad. In the case of the iPad being lost or stolen the iPad can be locked, wiped, tracked, and traced.

Acceptable Use

In addition to the school's Policy on the Acceptable Use of IT, the School permits use of the iPads in a manner that supports the school's aims and objectives and is in line with all School Policies.

This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the user terms and conditions named in this policy, privileges may be terminated, access to the school's network may be denied, and the appropriate disciplinary action shall be applied in line with the school's Policy on the Acceptable Use of IT.

Parent / Guardian Responsibilities

Parents are expected to talk to their children about the values and standards that they should follow on the use of the Internet just as they do on the use of all media information sources such as television, telephones, movies, radio, iBooks etc.
Parents are expected to:

- Ensure that their child keeps their iPad safe and uses it in accordance with the school procedures outlined in this document.
- Ensure that their child uses their device in accordance with school policies.
- Allow their son/daughter to use their iPad at home to assist them with homework, coursework etc.
- To monitor and oversee iPad use within the home setting.
- To ensure their son/ daughter's online safety by supporting the guidance provided.

Pupils' Responsibilities

Pupils' responsibilities are to:

- Use their iPad in a responsible and ethical manner.
- Obey general School rules concerning behaviour and communication that apply to iPad and computer use.
- Use all computer resources in an appropriate manner so as to not damage school equipment.
- Maintain regular backups to One Drive of any schoolwork saved on their iPad
- Report any email containing inappropriate or abusive language or if the subject matter is questionable.

Pupil Activities Specifically Prohibited

In addition to the guidance outlined in the school's IT Acceptable Use Policy and eSafety Policy, pupils are not permitted to:

- Illegally install or transmit copyrighted materials.
- Change iPad settings (exceptions include personal settings such as font size, brightness, etc.). • 'Jailbreak' their iPad (exploit the flaws of a locked-down electronic device to install software).
- 'Sideload' apps from the internet or another device.
- 'Sideload' vault or ghost apps to keep content hidden.
- Use or access another student's iPad.
- Leave their device on the school premises overnight.
- Attempt to modify, upgrade or repair iPads issued under this policy.
- Send or display offensive messages or material.
- Use obscene language or content.
- Use their iPad in a manner that causes damage to devices, computer systems or computer networks.
- Use other people's passwords to access online content.
- Trespass in others' folders, works or files.
- Download illegal content or material that is suspicious.
- Attempt to harm or destroy hardware, software, or data, including, but not limited to, the uploading of computer viruses or computer programs that can infiltrate computer systems.

- Transmit and access materials that are obscene, pornographic, offensive, threatening or otherwise intended to harass or demean recipients.
- Bypass the web filter by means of a web proxy.

Staff Responsibilities

We expect our staff to:

- Use the iPad in the classroom to enhance the teaching and learning experiences for their pupils.
- Follow relevant policies and procedures, particularly those regarding safeguarding.
- To be role models, display good practice and provide leadership in the use of these devices.

Legal Propriety

- Pupils should comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If a student is unsure, he should ask a teacher or parent.
- Use or possession of hacking software is strictly prohibited. Violation of the law may result in criminal prosecution or disciplinary action.

iPad Policy

I hereby confirm that I have read and understood the Pupil iPad Acceptable Use Policy and that I agree to abide by the requirements of the policy. I understand that failure to comply may result in the removal of the device supplied for my use and in certain circumstances may result in disciplinary action. I understand that the device has been supplied for educational purposes as specified by the school and that its return may be requested at any time. I understand that the device detailed below, its case and a genuine Apple charger and lightening cable must be returned to the school when I leave.

Pupil Name:	
Pupil's Signature:	
Parent's Name:	
Parent's Signature:	
Date:	
iPad Model:	
iPad Serial Number:	
Device Name:	
Head of IT Signature:	
Date:	

Appendix P

Online Safety Incident Report Form

Details of Incident *[This section to be completed by the person reporting the incident]*

Date: _____

Time: _____ am / pm.

Name of person reporting the incident: _____

Where did the incident occur?

- ☐ In School
- ☐ Outside of School

Who was involved in the incident? (Please give names)

- ☐ Pupil(s) _____
- ☐ Staff Member(s) _____
- ☐ Other (Please specify) _____

Type of incident:

- ☐ Bullying or harassment (cyber bullying)
- ☐ Deliberately bypassing security or access
- ☐ Hacking or virus propagation
- ☐ Racist, sexist, homophobic, religious hate material
- ☐ Terrorist material
- ☐ Drug / Bomb making material
- ☐ Child abuse images
- ☐ On-line gambling
- ☐ Soft core pornographic material
- ☐ Illegal hard core pornographic material
- ☐ Other (Please specify) _____

Description of incident (Include website url's or search criteria if relevant):

_____

_____

_____

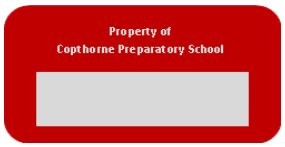
_____

_____

_____

Was School owned equipment used?

- ☐ Yes (If Yes, please give the asset label code if known)
- ☐ No



In your opinion was the incident deliberate or accidental?

- ☐ Deliberate
- ☐ Accidental

Did the incident involve material being?

- ☐ Created
- ☐ Viewed
- ☐ Printed
- ☐ Shown to others
- ☐ Transmitted to others
- ☐ Otherwise distributed

Could the incident be considered as?

- ☐ Harassment
- ☐ Grooming
- ☐ Cyber bullying
- ☐ Breach of 'Acceptable Use Policy'

Signed: Print Name:

Date:

Please hand this form to M Bone the nominated Online Safety Officer at the earliest opportunity

Action Taken *[This section to be completed by the Online Safety Officer or DSL]*

Staff

- ☐ Incident reported to:
  - ☐ Senior Leadership Team
  - ☐ Head of School
  - ☐ Chair of Governors
- ☐ Advice sought from the School's Legal Representative
- ☐ Incident reported to the Police
- ☐ Incident reported to the Internet Watch Foundation / CEOP
- ☐ Incident reported to social networking site
- ☐ Incident reported to IT Department
- ☐ Disciplinary action to be taken (Please specify)

  _____
- ☐ Online Safety Policy to be reviewed / amended

Please detail any specific action taken (ie. securing of equipment, printing of logs etc.)

_____

_____

_____

Pupil

- ☐ Incident reported to:
  - ☐ Designated Safeguarding Lead
  - ☐ Head of School
- ☐ Advice sought from Designated Safeguarding Lead
- ☐ Referral made to Local Authority
- ☐ Incident reported to the Police
- ☐ Incident Reported to the Internet Watch Foundation / CEOP
- ☐ Incident reported to social networking site
- ☐ Incident reported to IT Department
- ☐ Child's parents informed

- ☐ Child debriefed
- ☐ Disciplinary action to be taken (Please specify)

  _____

- ☐ Online Safety Policy to be reviewed / amended

Please detail any specific action taken (ie. securing of equipment, printing of logs etc.)

_____

_____

_____

Outcome of Incident / Investigation:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

A copy of this document should be held on file by the designated Online Safety Officer. A further copy should be attached to the Pupil's School Record or the Staff Member's Personnel File as deemed necessary by the Head of School / DSL / HR Department