COPTHORNE
PREPARATORY SCHOOL

ONLINE SAFETY POLICY 2024-25

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

Version:	One
Author:	Mr M Bone, Head of IT, DDSL (Online Safety Lead)
Reviewed:	June 2024
Review date:	September 2025
Approved by:	Mrs S Coutinho, Chair of Governors

1.1 Online Safety (e-Safety)

1.1.1 What is an e-Safety Policy?

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.

e-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 e-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 e-Safety policy 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 e-Safety policy is essential in setting out how we at Copthorne Preparatory School plan to develop and establish our e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

1.1.2 Other Relevant Policies

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.

Related policies include:

- Safeguarding Policy
- Data Protection Policy
- Data Retention Policy
- Curriculum Policy

1.2 Teaching and learning

1.2.1 Why is Internet use important?

The rapid developments in electronic communications are having many effects on our school community. It is important to state what we are trying to achieve in education through IT and Internet use.

- Internet use is an integral part of the current school curriculum at Copthorne Preparatory School and is a necessary tool for learning.
- Copthorne Preparatory School has a duty to provide pupils with quality internet access as part of their learning experience.
- Our pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
- The purpose of Internet use within school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

1.2.2 How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries.
- educational and cultural exchanges between pupils worldwide.
- vocational, social and leisure use in libraries, clubs and at home.
- access to experts in many fields for pupils and staff.
- professional development for staff through access to national developments, educational materials, and effective curriculum practice.
- collaboration across networks of schools, support services and professional associations.
- improved access to technical support including remote management of networks and automatic system updates.
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

Increased computer numbers and improved Internet access are both recent developments but their impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Our pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material must be taught and methods to detect plagiarism may need to be investigated.

- The school's Internet access is designed to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The Copthorne Preparatory School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Our pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Our pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

1.2.4 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent, and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for our pupils to develop skills in evaluating internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Our pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Our pupils will use age-appropriate tools to research internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

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.

1.3.2 How will email be managed?

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.
- Pupils in Y7 & 8 now have access to the 'Time to Talk' link on their iPads. The link connects to a Microsoft Office form where they can communicate directly with the DSL. Whilst not anonymous, it does allow for initial contact to be made any time, any day and from any location. All pupils will be

directed towards other existing methods of communication and the range of currently available websites with reporting capacity eg. Thinkuknow, Childline etc. This will be managed through our e-Safety lessons/curriculum.

1.3.3 How will published content be managed?

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 secure part of the website 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 headmaster 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.

1.3.4 Can pupils' images be published?

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 H).

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 e-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 E).
- 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 H).

1.3.5 How will social networking, social media and personal publishing be managed?

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 I) 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, instant messenger and many others.

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, IM and 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 I).

1.3.6 How will filtering be managed?

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.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.
- 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.
- Key loggers record all text sent by a workstation and analyse it for patterns.

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 are now reportable via 'MyConcern' if found to not be part of a legitimate lesson eg. Sex Education in Science, Drug Awareness in PSHE, eSafety 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 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 J) is continually reviewed.
- All breaches of filtering must be reported to the DSL and Head of IT immediately using 'MyConcern'. 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 Head of IT who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Surrey Police or CEOP.

1.3.7 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

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. Check who has signed into your meeting; as a guest without a camera would not be visible.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses must not be made available to other sites.
- Videoconferencing contact information must not be put on the school website.
- The equipment must be secure and if necessary locked away when not in use.
- 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.
- Only key administrators should be given access to videoconferencing administration areas or remote-control pages.
- When recording a videoconference lesson, written permission should be given by all sites and 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.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- 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.

1.3.8 How are emerging technologies managed?

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 G).

1.3.9 How should personal data be protected?

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 2018 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 2018 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.

Schools will already have information about their obligations under the regulations, and this section is a reminder that all data from which people can be identified is protected.

- Personal data will be recorded, processed, transferred, and made available according to the General Data Protection Regulations 2018.

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

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 authorised as a group.

Normally most pupils will be granted Internet access although Parental permission is sought before agreement is given (Appendix A/B/C/D). 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 F) 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 F)
- Parents will be informed that pupils will be provided with supervised 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 e–Safety rules and Acceptable Use Policy.

1.4.2 How will risks be assessed?

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 e–Safety policy is adequate and that the implementation of the e–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 1990 and breaches may be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any 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' and in any other relevant areas e.g. Bullying or Safeguarding log.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Safeguarding concerns, which will then be escalated appropriately.
- The school will manage e-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.

1.4.4 How will e–Safety incidents be handled?

Teachers and pupils should know how to report an eSafety incident (Appendix L). The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-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 school Designated Safeguarding Lead or e–Safety Coordinator. 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 headmaster and reported on 'Confide'.
- All e–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.

1.4.5 How is the Internet used across the community?

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket, or cybercafé. Ideally, young people would encounter a consistent internet use policy wherever they are.

Regarding internet access in the community, there is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance, filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g., social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

1.4.6 How will Cyberbullying be managed?

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.

1.4.7 How will Virtual Learning Environments be managed?

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.

1.4.8 How will mobile phones and personal devices be managed?

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.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

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

Consideration must be given as to the curriculum place for teaching e–Safety. Whilst the major role is taken by the IT Department as part of their e-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 e–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 e–Safety module will be included in the IT curriculum covering both safe school and home use.
- e–Safety training will be part of the transition programme when moving between sections of the school.
- e-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 e-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 How will the policy be discussed with 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 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.

1.5.3 How will parents' support be enlisted?

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.
- Interested parents will be referred to organisations listed in the "e–Safety Contacts" section.

1.6 e-Safety Contacts

CEOP (Child Exploitation and Online Protection Centre): https://www.ceop.police.uk/
Childline: https://www.childline.org.uk
Childnet: https://www.childnet.com
Cybermentors: https://www.cybermentorplus.org/
Digizen: http://old.digizen.org/
Internet Watch Foundation (IWF): https://www.iwf.org.uk/
Think U Know website: https://www.thinkuknow.co.uk/

1.7 Legal Framework

1.7.1 Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and staff should always consult with the relevant authorities if they are concerned that an offence may have been committed.

Many people use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.
It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).
Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

General Data Protection Regulations 2018
The regulations require anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The regulations also grant individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are

relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying policy.

Pupil 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.

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 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.

Please complete the sections on the next page to show that you have read, understood, and agree to the rules included in the Acceptable Use Agreement for your child. If you do not sign and return this agreement, then your child will not be able to make use of the school IT systems.

COPTHORNE
PREPARATORY SCHOOL

Pupil Acceptable Use Agreement Form - EYFS

This form relates to the Pupil Acceptable Use Policy - EYFS (Version X.X – XX/XX/XXXX), to which it was attached.

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, 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.

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

ONLINE SAFETY POLICY 2024 -25 – Appendix B

Pupil Acceptable Use Policy – PrePrep

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 PrePrep 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.

Please complete the sections on the next page to show that as a Parent/Carer you have read, understood, and agree to the rules included in the Acceptable Use Agreement for your child. If you do not sign and return this agreement, access will not be granted to school IT systems for your child.

COPTHORNE
PREPARATORY SCHOOL

Pupil Acceptable Use Agreement Form - PrePrep

This form relates to the Pupil Acceptable Use Policy - PrePrep (Version X.X – XX/XX/XXXX), to which it was attached.

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, 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:	

Pupil 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.

Please complete the sections on the next page 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, access will not be granted to school IT systems.

COPTHORNE
PREPARATORY SCHOOL

Pupil Acceptable Use Agreement Form - Prep

This form relates to the Pupil Acceptable Use Policy - Prep (Version x.x – xx/xx/xxxx), to which it was attached.

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, access will not be granted to school ICT 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, PDAs, 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:	

COPTHORNE PREPARATORY SCHOOL

ONLINE SAFETY POLICY 2024-25 – Appendix D

Parent/Carer Acceptable Use Policy Agreement - Prep

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. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

Permission Form

As the parent / carer of the pupil named below, I give permission 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, e-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:	

COPTHORNE PREPARATORY SCHOOL

ONLINE SAFETY POLICY 2024 - 25 – Appendix E

Use of Digital Images / Video Agreement – Whole School

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 sign 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 (delete as appropriate) 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.

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

Staff/Volunteer 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.

Acceptable Use Policy Agreement

I understand that I must use 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 e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the 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 permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only 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 have 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 (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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 Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

COPTHORNE
PREPARATORY SCHOOL

Staff / Volunteer Acceptable Use Agreement Form

This form relates to the Staff / Volunteer Acceptable Use Policy – Whole School (Version x.x – xx/xx/xxxx), to which it was attached.

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, 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, PDAs, 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, VLE, website etc.

Name:	
Signed:	
Date:	

Mobile Telephone 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 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 can be clearly identified and addressed, ensuring that the benefits that mobile phones 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 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 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.

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 only other exception to this rule is 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.

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 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

The school recognises the importance of emerging technologies present in modern mobile phones e.g., camera and video recording, internet access, MP3 and MP4 playback, blogging 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.

- 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, preferably the e-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 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.

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 Flickr to upload and share images of children with parents.
- The use of the system 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 to Flickr will only be taken on school devices.
- All users of Flickr 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

Social Media Policy

1. Introduction to the Policy

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 Management on how to deal with potentially inappropriate use of social networking sites.

2. 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.

3. 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 headmaster 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.

3. 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, Twitter and Instagram 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.

4. 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.

5. 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 headmaster 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 headmaster. However, staff must still operate in line with the requirements set out within the policy

6. 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 headmaster.
- 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.

7. 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, or Twitter 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.

8. 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, Director of Wellbeing, 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.

9. 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.

10. 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 management 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.

11. Child safeguarding guidance

If the Headmaster 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 their 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 Headmaster, 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

12. 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 schools 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.

13. Appendices

School staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

General Data Protection Regulations (EU) 2016/679

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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 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 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 e-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 e-safety awareness sessions.

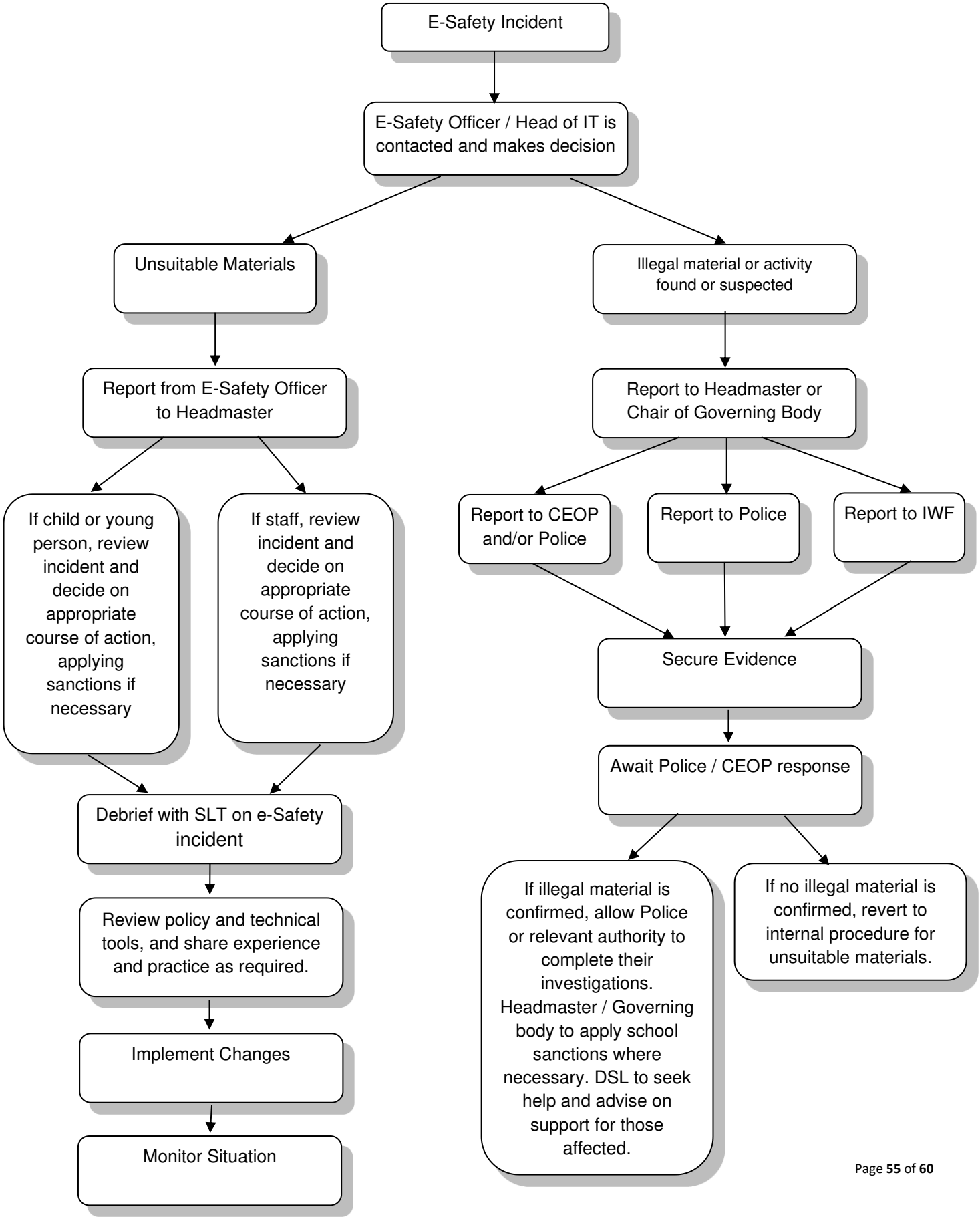
Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Head of IT who will decide in consultation with the Headmaster and/or Director of Studies what action is required.

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 E-Safety Policy and the Acceptable Use agreement.

COPTHORNE PREPARATORY SCHOOL

Appendix K **Flowchart for Responding to e-Safety Incidents**

(Adapted from BECTA model in AUPs in Context - Feb 2009)



COPTHORNE PREPARATORY SCHOOL

ONLINE SAFETY POLICY 2024 - 25 – Appendix L

---

eSafety 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):

_____

_____

COPTHORNE
PREPARATORY SCHOOL

_____

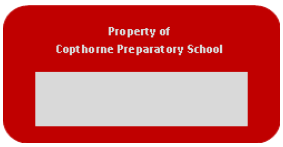
_____

_____

_____

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 D Bone the nominated eSafety Officer at the earliest opportunity

COPTHORNE PREPARATORY SCHOOL

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

Staff

- ☐ Incident reported to:
  - ☐ Senior Leadership Team
  - ☐ Headmaster
  - ☐ 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)

  _____
- ☐ eSafety Policy to be reviewed / amended

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

_____

_____

_____

Pupil

- ☐ Incident reported to:
  - ☐ Deputy Headmaster
  - ☐ Headmaster
- ☐ 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)

  _____
- ☐ eSafety 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 eSafety 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 Headmaster or DSL.

COPTHORNE
PREPARATORY SCHOOL

This policy will be reviewed annually by the Head of IT / DDSL (eSafety Lead)

Mark Bone
Head of IT

Reviewed: **June 2024**
Review date: **September 2025**