Internet and On-Line Safety Policy

This policy applies to all sections of Charlotte House School including EYFS.

Staff responsible:	SMT
Last review/update date:	January 2025
Review cycle:	Annually
Reviewed by Committee:	Ed Com
Approved by Board of Governors:	March 2025
Next review date:	Feb 2026
Related policies:	Anti-Bullying Policy Child Safeguarding Policy PSHEE Policy ICT Staff Acceptable Use
This document also appears on:	Website

In compliance with:

- DfE, Keeping Children Safe in Education, 2024
- ISI, Inspection Framework for the inspection of association independent schools, including residential boarding schools and early years settings, effective from 1 September 2023 (ISI Framework)
- ISI, Handbook for the inspection of association independent schools, including residential boarding schools and registered early years settings (ISI Handbook)
- DfE, Relationships Education, Relationships and Sex Education (RSE) and Health Education, Statutory guidance for governing bodies, proprietors, head teachers, principals, senior leadership teams, teachers (RSE Guidance)
- DfE, Behaviour in schools Advice for headteachers and school staff (Behaviour Guidance)
- DfE, Generative artificial intelligence (AI) in education – Policy Paper
- https://www.getsafeonline.org/
- Childnet International
- UK Safer Internet Centre - a partner of Childnet International, South West Grid for Learning and the Internet Watch Foundation: co-funded by the European Commission's "Safer Internet Programme"
- Child Exploitation and Online Protection Centre – a National Crime Agency command dealing with criminal / safeguarding concerns and reporting
- NSPCC, Keeping Children Safe Online
- Ofsted's Approach to Artificial Intelligence (AI) – Policy Paper
- *Working together to safeguard children (December 2023)*
- *Keeping Children Safe in Education (Sep 2024)*
- *Meeting digital and technology standards in schools and colleges (updated January 2024)*

1. Aims and Objectives

It is the duty of Charlotte House Prep to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy [(for all staff, visitors and pupils)], is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct;
- Behaviour Policy
- Data Protection Policy and Privacy Notice/s;
- School Trips Policy
- PSHE / RSE Policy; and
- Acceptable Use of AI

At Charlotte House Prep we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff, governors, and volunteers;
- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Safeguarding and Child Protection Policy as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the Online safety Coordinator, DSL and Senior Leadership Team are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for

procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at Charlotte House Prep. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Headteacher and Senior Leadership Team, Online Safety Co-ordinator and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that [termly] checks are properly made of the system.

3.4. Online Safety Coordinator

The DSL is the school's Online Safety Coordinator. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. They will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the SLT.

3.5. IT staff

The school's IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT.

3.6. Teaching and support staff

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Headteacher as appropriate.

3.7. Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

3.8. Parents and carers

Charlotte House Prep believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will

contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

Charlotte House Prep aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Coordinator will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding governor and the DSL/ Online Safety coordinator will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content and various adult content. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the Online Safety Coordinator/ DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, the Online Safety Coordinator / IT Staff will monitor the reporting logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Online Safety Coordinator/DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. [If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.]

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the Online Safety Coordinator if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate by clicking on the BEESAFE icon on their screen and then alert the member of staff they are with. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils are aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact a member of the IT staff for assistance.

5. Education and training

5.1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All teaching staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils can report concerns to the DSL/Online Safety Coordinator and any member of staff at the school.

Upper Prep Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Anti Bullying, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore shares the Hertfordshire termly online safety newsletter with parents and includes any pertinent information in the newsletter when there are local are national issues.

6. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the staff code of conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Charlotte House Prepare permitted to bring in personal devices for their own use. Staff are not allowed to have their personal devices switched on in the classrooms during the working day. They may use such devices in the main school staffroom or office block.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use and Staff Code of Conduct.

Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they should be switched off once on the school site and handed in to the Office switched off and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the learning support teacher to agree how the school can appropriately support such use. The learning support teacher will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school. These devices must be linked to the school Wi-Fi during the time in school so they are being monitored and filtered along with all other devices.

7. Online Communications

Staff

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / alumni (i.e. pupils under the age of 21 who have left the school within the past 12 months) or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and alumni under 21. Under no circumstances may staff contact a pupil or parent / carer and alumni under 21 using a personal telephone number, email address, or other messaging system nor should pupils, parents and alumni under 21/ their parents / carers be added as social network 'friends' or similar.

Staff must immediately report to the DSL / Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the school secretary.

Pupils

All Prep pupils are issued with their own personal google classroom addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This may be regarded as safe and secure, and must be used for all school work assignments. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should speak to the subject teacher for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the Online Safety Coordinator / DSL.

8. Use of social media

Staff

Staff must not access social networking sites, personal email whilst teaching. Such access may only be made from staff members' own devices whilst in the staff room or Office block

When accessed staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Charlotte House Prep into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

Pupils

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

9. Data protection

Please refer to the Data Protection policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to the school's central server / Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the school secretary &/or Beebug in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school secretary.

10.Password security

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed rugularly;
- not write passwords down; and
- not share passwords with other pupils or staff.

11.Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

Parents may give consent for their child's image to be used. Please check with the Registrar when a new child starts as to whether permission has been given or not.[

12.Artificial Intelligence

Charlotte House Prep does not currently permit pupils to use of generative AI tools such as ChatGPT on school devices.

Staff are aware that personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

Staff are aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, staff should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources.

13.Misuse

Charlotte House Prep will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

14.Complaints

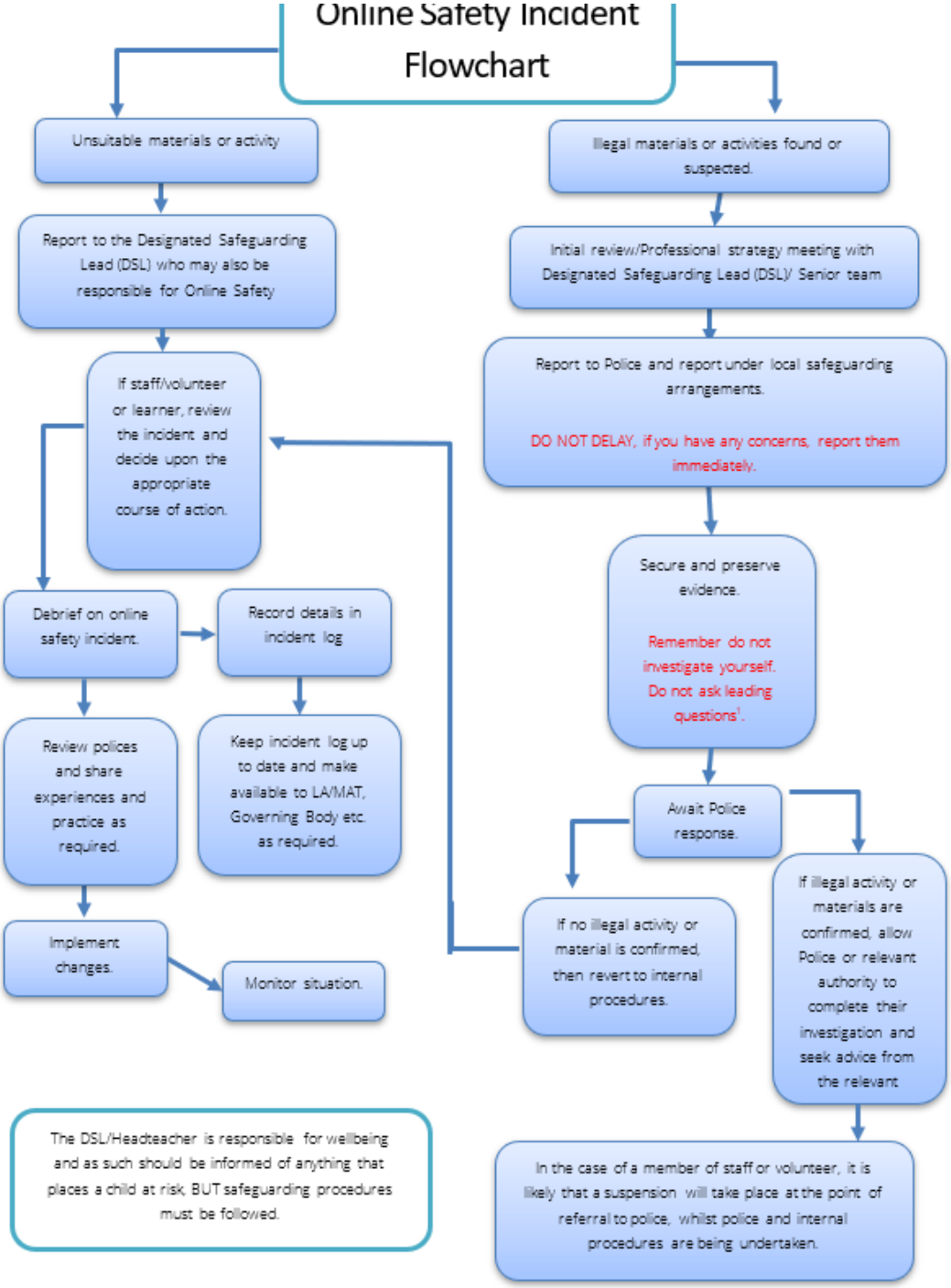
As with all issues of safety at Charlotte House, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Online Safety Coordinator in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's Online Safety Coordinator/ the DSL in accordance with the school's Safeguarding and Child Protection Policy.

Appendices

Appendix 1 Online Incident Flow chart
Appendix 2 Email / School Website Content/ Filtering Management/ IT System Security
Appendix 3 Risk Assessment/Staff Consultation/Internet Misuse
Appendix 4 Letter to EYFS/Pre-Prep Parents
Appendix 5 Letter to Prep School Parents
Appendix 6 Computer and Internet Rules (for pupils)
Appendix 7 Code of conduct for CharlotteHouse@home.

Appendix 1


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix 2 Email/Website/Filtering/Security

Email Management

Whole class or project email addresses may at times be used in school.

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in email communication.
- Access in school to external personal email accounts will be blocked if misused.

School Website Content

The school maintains its own dedicated website to provide information for current and prospective parents, pupils, staff and alumni.

- The point of contact on the school website is the school address, school email and telephone number. Staff or pupils' home information are not published.
- Website photographs that include pupils are selected carefully and do not enable individual pupils to be identified by any other means.
- Pupils' full names are not used anywhere on the school website, particularly associated with photographs. An exception to this is our secure parents' section of the school website where a username and password are required for access.
- Parents are given the opportunity in writing, to opt out of allowing photos of their children to be published on the school website.
- The Head or nominee takes overall editorial responsibility and ensures, as far as possible, content is accurate, appropriate and kept up to date.
- Certain information is shared with and/or links provided to other relevant websites, for example IAPS and search engines, for the purpose of effectively promoting the school.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.

Filtering Management

- The school works in partnership with parents and the school's IT Consultant to ensure systems to protect pupils are reviewed and improved.
- In the unlikely event that staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the IT Consultant via the Bursar. If a pupil has discovered the site, every effort is made to remove the view on the screen, whether by going 'Back' on the browser to the previously viewed page, or by turning the monitor off.
- The school seeks to ensure that regular checks are made to help us assess that the filtering methods selected are appropriate, effective and reasonable.

IT System Security

- The school IT systems are reviewed regularly with regard to security.
- Virus protection and firewall software is installed and updated regularly.
- Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to email.

Appendix 3

Risk Assessment

- In common with other media such as magazines, books and videos, some material available via the internet is unsuitable for pupils. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks are reviewed regularly.
- The Senior Management Team do everything within reason to assess that the **Internet and e-Safety policy** is implemented and compliance with the policy monitored.

Staff Consultation

- All staff must read and accept the ICT: Staff Acceptable Use Policy and agree to abide by the rules before using any internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, have access to the school **Internet and Online Policy**, and its importance explained. At least one staff INSET covering internet and online is held annually.
- The Head & Deputy Head as the DSLs keep all staff up to date with new legislation and advice from the government about e-Safety, on-line radicalisation and the issues of cyberbullying. This is an ongoing activity either through written correspondence or specific training sessions internally or with an outside supplier.
- Staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Internet Misuse

- Internet/email problems involving pupils, but originating out of school, will be investigated (as far as we legally can) if issues are brought into school and start to adversely affect behaviour or relationships. In such cases parents will be called in and appropriate action taken against offenders. Parents should, however, always alert the school to any problems in order that we can monitor behaviour and relationships between the pupils in school.
- Any instance of a child or parent posting defamatory or personal comments about the school, any member of staff, pupils or parents on any social media website, regular website or in any email brought to the school's attention, will result in the matter being vigorously investigated. Such conduct can lead to expulsion if the incident is deemed to be malicious and harmful to a child, an individual staff member or the school as a whole.
- Any member of staff who posts inappropriate comments or personal remarks about either a fellow staff member or a parent or child is subject to the school's internal disciplinary procedures. Where the Head deems it to be appropriate the individual concerned can be suspended on full pay pending any formal investigation.
- Issues and concerns must be reported to a member of the Senior Management Team. These will be reviewed and escalated as appropriate and may cross over into areas of general safeguarding of pupils and anti-bullying.
- Any complaint about staff misuse must be referred to the Head.

Appendix 4

Dear Parents

Responsible Computer and Internet Use for Pre-Prep Forms

As part of your child's curriculum and the development of ICT skills, Charlotte House School is providing supervised access to the internet. We believe that the use of the world wide web and email is worthwhile and is an essential skill for children as they grow up in the modern world.

We take very seriously the need to put safety procedures in place to protect the children, but we also expect the children themselves to be safe and responsible when using any ICT.

Please read and discuss the Computer and Internet Rules with your child and return the slip at the bottom of this page.

If you have any concerns or would like some explanation, please contact me.

Yours sincerely

Miss Penny Woodcock
Head

.....

Parent's consent for Computer and Internet Use

I have read and understood the school Computer and Internet Rules and give permission for my daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Child's name: _____ Class: _____

Signed: _____ Date: _____

Please print name: _____

Appendix 5

Dear Parents

Responsible Computer and Internet Use for Prep School Forms

As part of your child's curriculum and the development of ICT skills, Charlotte House School is providing supervised access to the internet. We believe that the use of the world wide web and email is worthwhile and is an essential skill for children as they grow up in the modern world.

We take very seriously the need to put safety procedures in place to protect the children, but we also expect the children themselves to be safe and responsible when using any ICT. As your child is entering the Prep School, there is an expectation that they will take more responsibility for their own actions in use of ICT and we are therefore now asking that they also sign the agreement slip below.

Please read and discuss the Computer and Internet Rules with your child and return the slip at the bottom of this page. The rules are printed overleaf for your future reference.

If you have any concerns or would like further explanation, please contact me.

Yours sincerely

Miss Penny Woodcock
Head

.....

Pupil's Agreement

- I have read and I understand the school Computer and Internet Rules
- I will use the computer, network, internet access and other new technologies in a responsible way at all times
- I know that network and internet access may be monitored

Name _____ Class _____ Signed _____

Parent's consent for Computer and Internet Use
I have read and understood the school Computer and Internet Rules and give permission for my daughter to access the internet.
I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.
I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Signed: _____ Date: _____

Please print name: _____

Appendix 6

Charlotte House Prep School
Computer and Internet Rules/ Cyber Safety Code

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the internet
- I understand that I must not bring software or memory sticks into school or download anything without permission
- I will only email people I know, or my teacher has approved
- The message I send will be polite and sensible
- I understand that I must never give my home address or phone number, or arrange to meet someone
- I will ask for permission before opening an email or an email attachment sent by someone I do not know
- I will not deliberately access data which belongs to someone else, whether pupil, teacher or other staff.
- I will not tell other people my ICT passwords
- I will not use internet chat facilities
- I will not deliberately look for, save or send anything that could be unpleasant.
- If I see anything I am unhappy with or I receive a message I do not like, I will click the bee icon on the screen and tell a teacher immediately
- I understand that the school may check my computer files and the internet sites I visit
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers and that further sanctions may be considered.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 7

Code of conduct for CharlotteHouse@home.

In order for digital home learning to be a safe learning experience, please ensure the following guidelines are observed:

- Zoom meets will be the main method of contact for the girls and their teachers. Parents should continue to communicate via e-mail.

- No parent or child is to invite a teacher to a Zoom meeting. All Zooms are to be initiated by Charlotte House Staff only in order to be in line with our safeguarding procedures. If you need to speak to a teacher then as before please email the teacher concerned who will schedule a time with you for a phone call.

- Zoom meets must take place in an open, shared, quiet space in your home. For safeguarding reasons, pupils should be dressed appropriately, and not be in a private area of the house (such as their bedroom). If possible they should be sitting at a table and be using a device they do not need to hold.

- When using Google Classroom the children are allowed to write comments on the stream which are directly linked to their learning but they should not write general comments. All children in the class can read the stream but for private direct messages about their learning, pupils should use the private comment on the class work assignment.

- On starting a Zoom meeting the girls will be in a 'waiting room' and the teachers will allow the girls in. By using this feature we ensure no one else can enter our meeting. Please ensure that the device is easily identifiable as your daughter's. All the girls will be muted and the teacher will unmute girls as and when it is appropriate. Girls will be expected to sit, listen and participate in the Zoom meets. If a girl continues to be disruptive during a lesson, despite being asked to stop, her video may be turned off and she will remain muted so she is not disturbing others; if this is the case the teacher will e-mail the parent after the lesson.

- All children should be monitored throughout their online learning activities. All links sent by staff have been fully vetted and any You Tube links have been routed through Safe Tube so should not include adverts and not move on to another video at the end. Some tasks will require the girls to research things; you may want to suggest to your daughter that she only uses the search engine https:// www.kiddle.co/as . Please discuss with your daughter what action you would like her to take if she does see something inappropriate on her screen - at school we talk about turning iPads so they are face down or turning screens off and then alerting an adult. We cannot stress enough the importance of reminding your children of on-line safety during any period of home learning. I am sure you are aware of the heightened risks at the moment that have been discussed on the

national news. https://www.thinkuknow.co.uk parents/ and https://www.childnet.com/parents-and-carers are great websites which may help you feel more able to discuss these matters with your daughter.

I am our Designated Safeguarding Officer and if you are worried that your daughter has seen any inappropriate images or been in any chat rooms please do let me know and I can suggest a course of action to support your daughter's mental well-being and her on-line safety.

Thank you once again for all you are doing to support your daughters at home. We will continue to work all together as a team to keep your daughters safe, happy and ensure they are continuing to soar like the skylark on our emblem!

Should you have any questions about our on-line code of conduct or e-safety please do contact me.

Best wishes

Penny Woodcock