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 2024
Review cycle:	Annually
Reviewed by Committee:	Ed Com
Approved by Board of Governors:	March 2024
Next review date:	Feb 2025
Related policies:	Anti-Bullying Policy Child Safeguarding Policy PSHEE Policy ICT Staff Acceptable Use
This document also appears on:	Website

In compliance with:

The use of social media for online radicalisation (July 2015)

Working together to safeguard children (December 2023)

Keeping Children Safe in Education (Sep 2023)
***Meeting digital and technology standards in schools and colleges** (updated January 2024)*

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

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 [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.

Internet Use - In School

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff, to enable on-line learning and to enhance the school's management information and business administration systems.
- The internet is an essential element in 21st century life for education. The school has a duty to provide children with quality, but safe internet access as part of their learning experience.
- As our own pupils are below the legal age for registering on social media sites such as Facebook, we discourage, through the wider curriculum, computing lessons and letters to parents, the use of any such sites by our children. Any sites categorised as social media are blocked for pupils by the firewall.

Internet Use - At Home

Parents are advised by the school to follow national guidelines on computer use by children at home and specifically, we strongly endorse the recommendation that children should not have unsupervised access to computers or mobile devices such as i-pads connected to the internet in their own room. During any extended period of on-line learning parents are reminded of the school's Zoom etiquette requirements and of the importance of actively monitoring their children's on-line activities. Parents are contacted by the Head if staff have reason to suspect a child is accessing inappropriate content at home.

Internet benefits to education

Benefits of using the internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Being able to continue educating pupils when they are off site

Internet use to enhance learning

- The school internet access is designed expressly for use in school and includes specific filtering for pupils appropriate to the age of pupils, using recognised security and virus software.
- Pupils are taught what is acceptable and what is not acceptable and given clear objectives for internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide pupils in online activities that support the learning outcomes planned for the pupils' age.
- Pupils are educated in the effective use of the internet in research, including the skills and value of information location and retrieval.
- Pupils are stimulated via a range of resources including 'live' lessons when learning remotely.

Internet Safety

The school has comprehensive technical provision in place to ensure the safety of pupils. These include anti-virus software, web-filtering software and classroom and desktop management software. The monitoring and filtering of the children's access to the internet is part of our safeguarding work as we must ensure they are not accessing information on-line which puts them physically or mentally in danger.

The school's web-filtering system blocks *most* 'unsafe' or 'undesirable' websites from the children's access. However, certain rules should be applied for times when that does not happen (See Appendix 1 & 2).

If staff discover unsuitable sites, the URL (address) and content is reported to the Head as DSL to make a decision regarding blocking the site and then to the school's IT consultant via the Bursar and/or the Head's PA. If pupils discover unsuitable sites they know to immediately alert the member of staff present who report the details as above. The Bursar, DSL and Head receive updates from SOPHOS with information relating to blocked and objectional domains.

Pupils, staff and parents are educated to understand how to use the internet safely. This takes place through dedicated lessons during the pupils' computing classes and e-safety talks presented to staff and parents. When appropriate, advice will also be sent out via email which includes termly newsletters for staff and parents produced by Herts For Learning. We have also signed up to The National College and National Online Safety which will help staff to stay up to date with their on-line safety knowledge but also provides a log on for parents so they can access training and information.

The school participates in Internet Safety Day every February which involves an assembly led by our computing co-ordinator. Year groups from Form I upwards have e-safety lessons planned to take place over the school year.

The Head, DSL & Bursar keep abreast of current issues and guidance and any changes are relayed to the staff/governors as appropriate, in order to update the school e-Safety teaching and policies accordingly. As appropriate, the information is then relayed to parents. See Appendix 3.

Issues arising from online activities that affect pupils and/or staff in the school, are immediately reported to the Bursar to action. Where these issues cross over into safeguarding matters for pupils, the school's **Safeguarding Policy** will come into force.

All parents (and prep school pupils) are asked to sign a form agreeing to Charlotte House Computer and Internet rules, before access to the internet is allowed. These incorporate measures to help ensure the e-safety of the pupils in school (See Appendices 4 & 5). Code of conduct for CharlotteHouse@home is applied during periods of on-line learning to complement e-safety (see Appendix 7).

The designated safeguarding lead (DSL) has responsibility for understanding the filtering and monitoring systems and processes in place as part of their remit as this is such a key issue as far as safeguarding is concerned. They work closely with Beebug, our IT advisors to ensure our system is at the right level and does not 'over-block'.

Authorised Internet access

All staff and pupils are granted internet access.

EYFS and Pre-Prep access to the internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials (e.g. Purple Mash).

Parents are informed that pupils will be provided with supervised Internet access.

Parents are asked to sign and return a consent form (See Appendices 3 & 4).

–How do our pupils know about this policy?

Rules for internet access are posted in the IT suite and in every classroom by the ipads (See Appendix 6)

Be SMART online safety posters are on display throughout the school.

Pupils are informed that Internet use will be monitored.

Instruction in responsible and safe use precedes internet access.

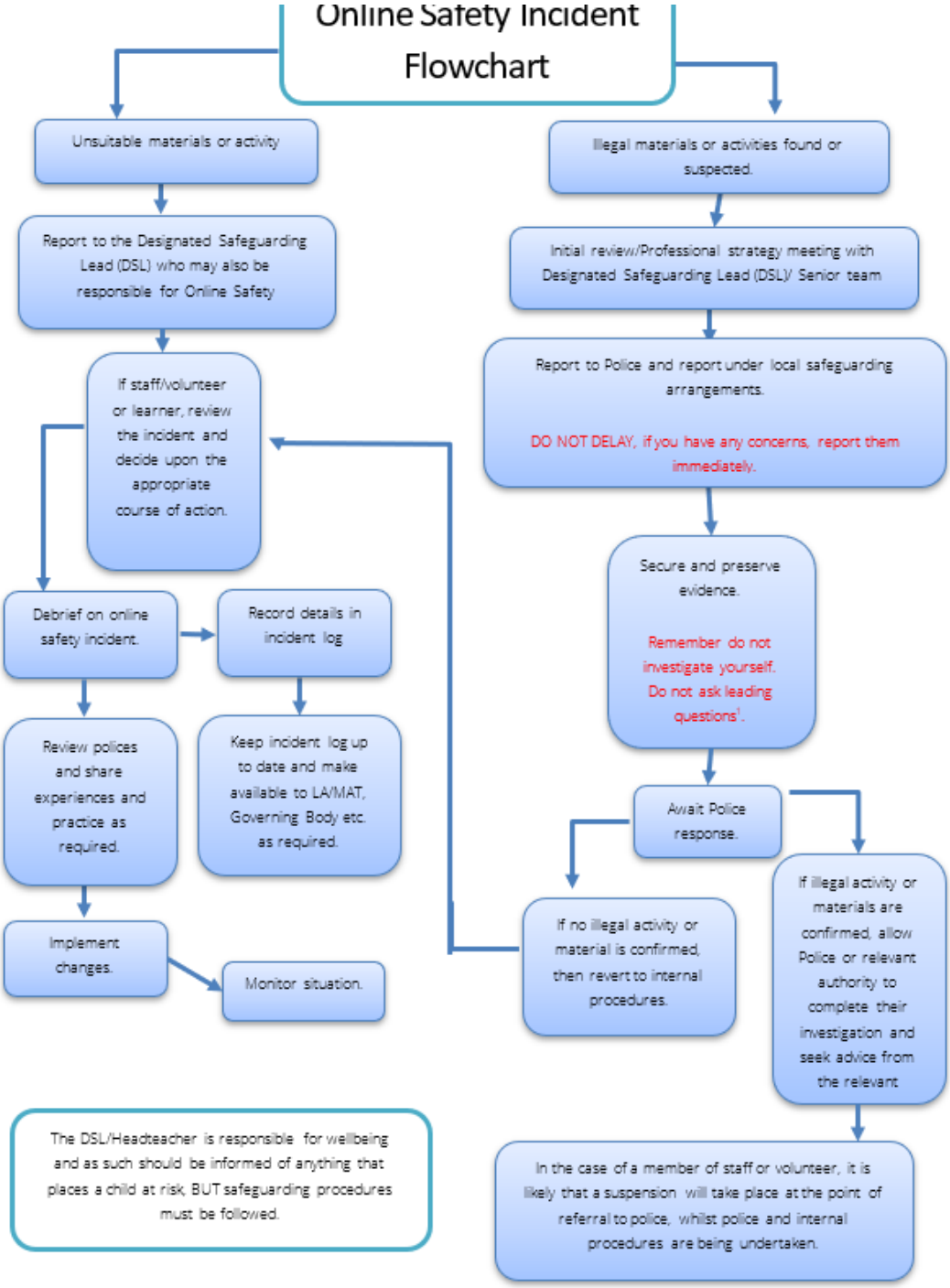
Zoom etiquette is shared with pupils in the first Zoom lesson of a period of on-line learning

During any extended period of on-line learning the girls will be periodically reminded of e-safety and before any research projects are set they will be reminded of 'safe' sites to use.

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 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