Online Safety Policy

Chepstow House School & Little Chepstow Nursery

Date of adoption of this policy	September 2026
Date of last review of this policy	August 2026
Date for next review of this policy	July 2027
Policy owner	**Designated Safeguarding Lead:** Karen Etherington Deputy Head (School) Telephone: 0207 2430243 mob: 07785627536 Email: dsl@chepstowhouseschool.co.uk **Designated Safeguarding Lead:** Gill Whiteside (Nursery) Telephone: 0207 2430243 Email: dsl@chepstowhouseschool.co.uk The **Deputy Designated Safeguarding Lead** can be contacted in the DSL"s absence. Sarah Egerton-Warburton Telephone: 0207 243 0243 Email: dsl@chepstowhouseschool.co.uk

Contents

1	Aims	3
2	Scope and application	3
3	Regulatory framework	3
4	Publication and availability	5
5	Definitions	5
6	Responsibility statement and allocation of tasks	5
7	Role of staff and parents	7
8	Technological controls	11
9	Procedures for dealing with online safety concerns and incidents	14
10	Education	17
11	Training	19
12	Risk assessment	23

1 Aims

1.1 This is the online safety policy of Chepstow House School (including Little Chepstow Nursery).

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

2.1.2 protects the whole School community from illegal, inappropriate and harmful content or contact;

2.2.2 educates the whole School community about their access to and use of technology;

2.3.2 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and

2.4.2 promotes a whole school culture of safety, equality and protection.

1.3 This policy forms part of a whole school approach to promoting child safeguarding and wellbeing, which seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout many of the School's policies and procedures (including its child protection and safeguarding policy and procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead.

2 Scope and application

2.1 This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

2.2 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014

3.1.2 Statutory framework for the Early Years Foundation Stage (DfE, September 2021)

3.1.3 Education and Skills Act 2008;

3.1.4 Education Act 1996 (as amended)

3.1.5 Education and Inspections Act 2006

3.1.6 Children Act 1989;

3.1.7 Childcare Act 2006;

3.1.8 Data Protection Act 2018, the Data (Use and Access) Act 2025 and UK General Data Protection Regulation (**UK GDPR**); and

3.1.9 Equality Act 2010.

3.1.10 In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping Children Safe in Education 2026 (DfE, Effective 1 September 2026) (**KCSIE**);

3.2.2 Preventing Bullying (DfE July 2026)

3.2.3 Sharing nudes and semi-nudes: how to respond to an incident (overview) (DfDCMS and UKCIS, March 2024);

Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) (DCMS and UKCIS, March 2024);

3.2.4 Revised Prevent duty guidance: for England and Wales (Home Office, 2023);

3.2.5 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, April 2025);

3.2.6 Searching, screening and confiscation: advice for schools (DfE, July 2023);

3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

3.2.8 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, December 2025);

3.2.9 Teaching online safety in schools (DfE, January 2023);

3.2.10 Harmful online challenges and online hoaxes (DfE, February 2021);

3.2.11 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021);

3.2.12 A business guide for protecting children on your online platform (DfDCMS, June 2021);

3.2.13 Online safety audit tool (UKCIS, October 2022);

3.2.14 Mobile phones in schools: statutory guidance (DfE, June 2026);

3.2.15 Generative AI: product safety expectations (DfE, January 2026);

3.2.16 Cyber security standards for schools and colleges (DfE, August 2026).

3.2.17 Meeting digital and technology standards for schools and colleges (DfE, August 2026)

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 acceptable use policy for pupils;

3.3.2 staff IT acceptable use policy and social media policies;

3.3.3 child protection and safeguarding policy and procedures, including guidance on child-on-child abuse;

3.3.4 anti-bullying policy;

3.3.5 risk assessment policy;

3.3.6 staff code of conduct;

3.3.7 Whistleblowing policy;

3.3.8 data protection policy;

3.3.9 Mobile Phones and Electronic Devices Policy;

3.3.10 Behaviour, Discipline and Exclusion policy;

3.3.11 Chepstow House school rules;

3.3.12 Relationships, Health and Sex education policy.

3.3.13 Complaints Policy & Procedure

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request. It can be made available in large print or other accessible format if required.

5 Definitions

5.1 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6 Responsibility statement and allocation of tasks

6.1 Inspired Education Group has overall responsibility for all matters which are the subject of this policy. It ensures that all those with leadership and management responsibilities at the School actively promote the well-being of pupils.

6.2 The Designated Safeguarding Lead (**DSL**; see cover page for contact details) has primary responsibility for the implementation and maintenance of this policy at school level. The policy is updated as required and formally reviewed on an annual basis. The policy will also be reviewed if:

6.2.1 A safeguarding risk is identified;

6.2.2 There is a change to working practices;

6.2.3 New technology is introduced (e.g. new devices);

6.2.4 Major software updates occur; or

6.2.5 There are changes to the technical configurations of the network and devices.

6.3 Online safety incidents are reviewed as part of an ongoing cycle of governance visits, and as part of an annual safeguarding review conducted by the Nominated Safeguarding Governor and DSL. Governors regularly review the effectiveness of school filters and monitoring systems in termly governance visits. Staff online safety and safeguarding and child protection training ensures they have an understanding of the expectations, roles and responsibilities around the setting's filtering and monitoring system. The Governors have reviewed the DFE's Meeting digital and technology standards in schools and colleges and have discussed its content with the IT department to ensure standards are met. The Governors also consider the age, number of pupils and those who are potentially at a greater risk of harm, when limiting children and young people's exposure to risk.

6.4 The Governors receive termly reports at governors' meetings regarding the effectiveness of filtering and monitoring systems, significant online safety incidents, emerging risks, and actions taken to address identified safeguarding concerns.

6.5 In addition any significant or serious online safety incidents are immediately reported to the Safeguarding Governor

6.6 The effectiveness of the School's filtering and monitoring systems will be formally reviewed at least once every academic year. This review is separate from, and in addition to, the routine technical security checks carried out by the IT team. The review will consider whether the systems remain appropriate to the age range, number and vulnerability of pupils at the School, and whether they strike the right balance between safeguarding and unreasonable over-blocking of legitimate educational content. The outcome of this review, including any actions identified, will be recorded and reported to the Governing Body.

6.7 Taking into account the multi-dimensional aspects of online safety, specific responsibilities are assigned to specific individuals based on their skills and experience, as set out below:

Aspect of online safety	Designated person
Senior Leadership Team Lead for filtering and monitoring	Karen Etherington
ICT Coordinator	Collette Pearce
On-site Engineer[1]	Inspired Education Group
Curriculum - ICT	Collette Pearce

[1] The on-site engineer must sign the annual affirmation statement as required by the Code of Ethical & Professional Conduct.

Curriculum - PSHEE	Karen Etherington & Alex Hunter
Staff Training & CPD	Sabrina Morse
Development of Parental Awareness	Collette Pearce

7 Role of staff and parents

7.1 Head and Senior Leadership Team

7.1.1 The Head has overall executive responsibility for the safety and welfare of members of the School community.

7.1.2 The DSL is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the DSL includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's child protection and safeguarding policy and procedures.

7.1.3 The DSL will work with the School's On-Site Engineer and ICT Coordinator (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.1.4 The DSL will monitor the School's online safety incident log.

7.1.5 The DSL, who leads on online safety and has a lead responsibility in understanding the filtering and monitoring systems (which is explicit in the job description), will regularly run reports using the filtering software to identify risk alerts and concerns.

7.1.6 The DSL will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

7.1.7 A member of the Senior Leadership Team has been given specific responsibility for filtering and monitoring, including leading the annual effectiveness review required under KCSIE. This person is the DSL, who also provides safeguarding input, and is supported by the IT team, who provide technical input.

7.2 Inspired Director of IT and IT Team

7.1.1 Inspired IT, together with his team of On-Site Engineers, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including illegal child abuse material, unlawful terrorist and extremist content and adult content, while using the School's network. This includes responsibility for ensuring that:

a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack, and that such safety mechanisms are updated regularly;

b) conducting a full security check and monitoring the school's ICT systems on a termly basis;

c) blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

d) the user may only use the School's technology if they are properly authenticated and authorised;

e) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;

f) the School has used the DFE's 'plan technology for your school' service, to self-assess against the filtering and monitoring standards;

g) the School has taken appropriate action to meet the DfE's Cyber Security Standards, to improve resilience against cyber-attacks;

h) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

i) managing the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls;

j) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

k) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

7.1.2 Whilst the above responsibilities sit with the Inspired IT and are administered by the School's On-Site Engineer, it is essential that a member of staff is nominated as ICT Coordinator and is assigned responsibility for monitoring the effective delivery of technology services on behalf of all school users, and for reporting problems where necessary. The ICT Co-ordinator may also be responsible for the ICT curriculum, but it is important that these two responsibilities are clearly understood as separate functions.

7.1.3 The ICT Coordinator will report regularly to the Senior Leadership Team on the operation of the School's technology. If the ICT Coordinator has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the DSL and Inspired Group's Head Office IT team.

7.1.4 The ICT Coordinator is responsible for bringing any matters of safeguarding concern to the attention of the DSL in accordance with the School's child protection and safeguarding policy and procedures.

7.2 All staff

7.2.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

7.2.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.2.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face, inside and outside of school. Staff are also aware that in many cases such abuse will take place concurrently both online and offline. All staff understand the risk of harm and indicators of abuse and neglect.

All staff are aware that children can abuse other children at any age (child-on-child abuse) and this can happen both inside and outside of school and online. Staff are expected to be alert to this possibility online (technology is a significant component in safeguarding and well-being issues) and are aware of the policies and procedures in place and the role they hold in preventing and responding to a child who is believed to be at risk. All staff should report any concerns, no matter how small, to the DSL.

Examples of such abuse can include:

a) the sending of abusive, harassing and misogynistic/misandrist messages;

b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

c) the sharing of abusive images and pornography to those who do not wish to receive such content;

d) cyberbullying.

7.2.4 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

a) facilitates, threatens and/or encourages physical abuse;

b) facilitates, threatens and/or encourages sexual abuse/violence and sexual harassment;

c) is used as part of initiation/hazing type violence and rituals; or

d) Abuse (including sexual) can also be wholly online and/or technology facilitates offline abuse.

7.2.5 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.2.6 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. The School has a **zero tolerance approach** towards child-on-child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour and discipline policy and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures.

7.2.7 Staff are aware of and have an understanding of the systems in place and know how to escalate concerns. They have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's child protection and safeguarding policy and procedures. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the DSL in all cases (see contact details on cover page).**

7.2.8 Staff authorised by the Head have the right to search for, examine and confiscate any device where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. This will be done in accordance with the Department for Education's guidance: Searching, screening and confiscation (July 2023). Inappropriate usage will be dealt with consistent with the School's policy on behaviour and discipline. Following an examination of an electronic device, the member of staff has the right to erase any data or files, if they think there is a good reason to do so. However, care should be taken not to delete material that might be required in a potential criminal investigation.

7.2.9 If a member of staff has reasonable grounds to suspect that a device contains evidence in relation to an offence, they must alert the Head and, where there are safeguarding concerns, the DSL. In relevant cases the head / DSL should follow the guidance: Sharing nudes and semi-nudes: how to respond to an incident (overview) (DfDCMS and UKCIS, March 2024); and in other cases which may constitute a crime, the Head / DSL should take advice from the police regarding seizure, handing to the police / storage and / or deletion of any content. This includes images or videos that have been digitally altered or wholly generated using artificial intelligence (including so-called "deepfakes"), which are treated in the same way as genuine images for the purposes of this policy.

7.2.10 A conviction of a child, parent or family member has the possibility to generate interest among students in school (even with legal anonymity reporting restrictions). It is important that the victim and perpetrator(s) are protected by the school, especially from harassment or bullying (online included). Social media is likely to play a key role following an incident/alleged incident. The victim and alleged perpetrator(s) can be in contact, as well as friends from both sides who could harass the students online and/or become victims of harassment themselves.

7.3 Parents

7.3.1 The role of parents and carers in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents and carers to promote safe practice when using technology and to:

a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

d) Understand how access to 4/5G or VPNs can be used to circumvent filtering and monitoring systems, both at home and at school and enable access to concerning / illegal material on-line.

7.4.2 If parents have any concerns or require any information about online safety, they should contact the DSL.

8 Technological controls

8.1 We maintain specific controls which enable us to establish a secure data and communications environment and to monitor children's digital activity within the boundaries of the School.

8.2 Children to whom we provide bespoke[2] access to ICT resources are asked to agree in writing to a set of rules for the acceptable use of such resources (see ICT Usage policy).

8.3 Our password-controlled network maintains individual security, confidentiality and accountability for activity on the network. Any pupil or member of staff who has a problem with their user names or passwords must report it to the School's ICT team immediately.

8.4 The School uses well-established and frequently updated filtering software to prevent access to content deemed to be potentially harmful, and which records attempts to access such potentially harmful content. If staff or children discover unsuitable sites, the URL (web address) must be reported to the ICT Coordinator. Any member of the School community should report a website which causes concern to the ICT Coordinator who will immediately refer this to the On-Site Engineer who will arrange for that site to be blocked, always taking care to consider that potential 'over-blocking' does not lead to unreasonable restrictions in online learning.

8.5 The use of any device connected to the School's network will be logged and monitored by the ICT team.

8.6 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the ICT team.

[2] E.g. email accounts; network ID's and accounts; unsupervised browsing

8.7 Inappropriate material

8.7.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

8.7.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the DSL. The term 'online safety' encapsulates a wide range of issues but these can be classified into four main areas of risk

a) **Content** - being exposed to illegal, inappropriate, or harmful content (e.g. pornography, racism, extreme violence, addictive content, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories[3];

b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, bullying, harassment, threats to privacy, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);

c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images/videos (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, harassment, breaching copyright); and

d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If pupils, students or staff are at risk, it should be reported to the Anti-Phishing Working Group (https://apwg.org/).

The school is committed to supporting awareness of these risks in age-appropriate ways and to building resilience and critical thinking skills to enable students to respond appropriately to such risks. See the table below (adapted from Tanya Byron's '3 C's of E-safety') and section 10 for further information about online safety education.

[3] Online games designed for adults are often cited as one of the principle causes of concern for several of these risks. This may be as much from the highly aggressive and verbally abusive behaviours they elicit as from the be-friending of pseudonymous strangers or from exposure to violent and sexual content. Extensive exposure to such games may be considered evidence of child neglect, which may, in certain circumstances, lead the School to consider making a report to social services.

Risk category	Commercial	Aggressive	Sexual	Values
Content Child is observer/consumer	Understand and develop resilience to advertising, spam, sponsorships and demands for personal information	Develop resilience to violent/hateful content and know how to cope and to deal with it	Avoid/develop resilience to pornographic or unwelcome sexual content	Develop critical evaluation skills to Identify bias, prejudice, misleading and manipulative information and advice
Contact Child is participant	Awareness of tracking, harvesting and the protection of personal information	Develop resilience to being bullied or harassed, and know what actions to take	Understand the implications of interacting with strangers and being groomed	Develop resilience to the risk of compulsive/addictive online behaviour, and to unwelcome persuasions
Conduct Child is instigator/perpetrator	Clear guidance on illegal downloading, copying, plagiarising, hacking, gambling, fraud, identity theft and the consequences	Clear guidance on bullying, harassment or 'trolling' of others and understand the consequences	Clear guidance on creating and uploading inappropriate material and understand the consequences	Clear guidance on the value of personal integrity, respect, data security, confidentiality, and the consequences of publishing inappropriate, false or misleading information or advice

8.8 Use of mobile electronic devices and smart technology

8.8.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet, social media and communication network sites when connected to the School's network. Pupils are not allowed access to a mobile phone during the school day and are not allowed to access the internet, other than via the school's network, on an authorised school or BYOD device. The School operates a clear mobile phones and electronic devices policy and has mechanisms in place to manage such risks.

8.8.2 Within school children have access to school IT devices, if any personal devices are brought into school children follow the procedures set out in the school mobile phones and devices policy. School devices are connected to the school Wi-Fi and children are taught online safety in lessons throughout the year.

8.8.3 The School operates a mobile phone policy designed to safeguard pupils and promote a positive learning environment. Pupils may not use mobile phones or other internet-enabled smart devices during the school day unless specifically authorised by a member of staff for educational, medical or safeguarding purposes.

8.8.4 The School recognises that mobile data connections, VPNs and personal hotspots can bypass filtering and monitoring systems and therefore prohibits their use where this would circumvent School safeguards. Any misuse of mobile phones, smart technology or internet-enabled devices will be dealt with under the School's behaviour policy and, where relevant, the School's child protection and safeguarding procedures. Further details are set out in the School's Mobile Phone and Electronic Devices Policy.

8.8.5 The use of mobile electronic devices by staff is covered in the code of conduct, Staff IT acceptable use polices, social media policy, mobile phone and devices policy and data protection policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

8.8.6 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

8.8.7 The school is aware of the risk of children being exploited into county line practices (increasingly targeted and recruited through social media).

8.8.8 Pupils deliberately acting outside of this guidance, for example, whilst at school using VPNs or 4/5G to access the internet will be regarded as a behaviour / discipline issue.

8.8.9 The School's filtering and monitoring systems are kept under review to reflect the risks posed by generative AI tools, including their capacity to produce real-time, dynamic and personalised content that traditional URL-based filtering cannot always detect. Only AI tools approved by the School may be used on School devices, networks or accounts

9 Procedures for dealing with online safety concerns and incidents

9.1 Concerns/Incidents relating to pupils

9.1.1 **Anyone** who has **any** concern about pupils' online safety, the misuse of technology or a particular risk should report it immediately.

a) If a concern or incident in any way touches on child safeguarding issues[4], then it must be reported **immediately** to the DSL, consistent with the safeguarding and child protection policy.

b) If the concern or incident involves cyberbullying it should be dealt with in accordance with the School's anti-bullying policy.

c) If it relates to technological controls (as described above), or to a breach of the ICT Usage policy, then it must also be reported to the ICT Coordinator.

d) Other members of staff and management should be informed as appropriate in the circumstances.

9.1.2 Regarding the responsibility of schools to deal with online safety incidents which occur 'off-site', the Education and Inspections Act 2006 and the Education Act 2011 empower the School, to such extent as is reasonable, to:

(a) regulate the behaviour of children when they are off the school site where an online safety incident is linked to the school

[4] For example, it involves child-on-child abuse, sexual imagery, sexual violence and/or harassment, upskirting or radicalisation (this is not an exhaustive list, for further information see the safeguarding and child protection policy).

(b) impose disciplinary penalties for inappropriate behaviour, as per the behaviour and discipline policy

(c) search for and confiscate electronic devices, and search their contents, and where appropriate delete content (see section 7.3.8)

9.1.3 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously and equally, whether online or outside of school. Children should never have the impression that they are creating a problem through reporting violence or harassment. It is key to explain that the law is in place to protect them, not criminalise them (explained without causing alarm or distress). Staff should however be careful not to promise full confidentiality as information may need to shared further (e.g. with the DSL) to determine next steps.

9.2 Concerns/Incidents relating to staff

9.2.1 **Anyone** who has **any** concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.2.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should report it **immediately** in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's child protection and safeguarding policy and procedures.

9.3 Misuse by any user

9.3.1 **Anyone** who has **any** concern about the misuse of technology by any other user should report it immediately to the ICT Coordinator and/or the DSL as relevant.

9.3.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.3.3 If the School considers that any person is vulnerable to radicalisation, the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

9.4 Concerns relating to the filtering / monitoring system

9.4.1 All staff should report to the DSL and the IT Coordinator if there is a failure in the filtering and monitoring systems; abuse of the system or if they notice abbreviations or misspellings that allow access to restricted material.

9.4.2 All staff should report to the DSL and the IT Coordinator if there are perceived unreasonable restrictions that affect teaching, learning or administrative tasks.

9.4.3 All staff should report to the DSL and the IT Coordinator in advance if they are teaching topics which could create unusual activity on the filtering logs.

9.5 Cybercrime

9.5.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

9.5.2 Cyber-dependent crimes include;

(a) unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

(b) denial of service (Dos or DDoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

(c) making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

9.5.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

9.5.4 If staff have any concerns about a child in this area, they should refer the matter to the DSL immediately. The DSL should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general online safety.

9.6 Recording online safety incidents

The School maintains a log of online safety incidents, which is monitored by the DSL. The reporting of online safety incidents should include the following data:

(a) Name of person reporting the incident

(b) Date and time of incident

(c) Date reported

(d) Names of people involved

(e) Location and device details

(f) Details of incident, including evidence where possible

(g) Clarification of the risk or breach – e.g. does it relate to safeguarding, bullying, inappropriate content, sexting, data protection, copyright infringement…etc.? Use the 4 C's categorisation as described in 8.7.2.

(h) Initial action taken and current status

9.7 Once investigated, a record of the resolution of the incident, and actions taken as a result, must be maintained. Such records should be readily available for inspection during governance visits.

9.8 The information created in connection with this policy may contain personal data. The School's use of this personal data will be in accordance with Inspired Education Group's data protection and retention policies. Data in the online safety log will be processed in line with Inspired Education Group's Privacy Notice, which is available on request or can be accessed via the SharePoint.

10 Education

10.1 The safe use of technology is integral to the School's curriculum. Governors ensure pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices school's curriculum and PSHE policies. The education will be tailored to the specific needs and vulnerabilities of individual children, including those who with special education needs or disabilities and those who are victims of abuse. It is understood that children with specific needs can face additional safeguarding challenges both in-person and online. Governors recognise the barriers, including cognitive understanding.

10.2 We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate.

10.3 We believe that the internet and the constantly evolving technologies and devices to which children have access can be tools that enrich their lives. We therefore teach them to view technology and new media positively whilst simultaneously protecting themselves.

10.4 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:

10.4.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.4.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

10.4.3 to be critically aware of content they access online and guided to validate accuracy of information;

10.4.4 how to recognise suspicious, bullying or extremist behaviour;

10.4.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.4.6 the consequences of negative online behaviour;

10.4.7 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

10.4.8 how to respond to harmful online challenges and hoaxes but staff must be mindful that openly naming harmful sites, to either parents or pupils, can encourage interest from pupils who otherwise may not have known about the sites existence.

10.4.9 how generative AI works, its limitations and risk of producing inaccurate, biased or misleading information; the risks of AI-generated deepfakes and manipulated images, including in the context of sharing nudes and semi-nudes; the privacy implications of interacting with AI systems; and the ethical use of AI in learning, coursework and assessment.

10.5 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element.

10.6 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

10.7 The School's acceptable use policy for pupils sets out the School rules regarding the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

10.8 Technology is included in the educational programmes followed in the EYFS in the following ways:

10.8.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

10.8.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

10.8.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.]

10.9 Useful online safety resources for pupils

10.9.1 http://www.thinkuknow.co.uk/ (also provides support for parents and carers)

10.9.2 http://www.childnet.com/young-people

10.9.3 https://childnet.com/resources/smartie-the-penguin]

10.9.4 https://www.childnet.com/resources/digiduck-stories]

10.9.5 https://www.saferinternet.org.uk/advice-centre/young-people

10.9.6 https://www.disrespectnobody.co.uk/

10.9.7 https://mysafetynet.org.uk/

10.9.8 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

10.9.9 https://www.bbc.com/ownit

10.9.10 https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

10.9.11 Childline | Childline

10.9.12 Report Harmful Content - We Help You Remove Content

10.9.13 CEOP Safety Centre

11 Training

11.1 Staff

11.1.1 The School provides training on the safe use of technology to staff (online safety as part of required safeguarding training and child protection training) so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur. Training is regularly updated and staff should receive child protection and safeguarding updates through meetings and emails, as required and at least annually, to provide them with the knowledge to effectively safeguard children.

11.1.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy. New staff will receive training to understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

11.1.3 Ongoing staff development training includes training on technology safety together with specific safeguarding issues such as sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. Updates on online safety issues are shared as required and at least annually via emails and staff meetings.

11.1.4 Staff training includes safeguarding risks associated with generative AI, including recognising AI-generated or deepfake sexual imagery involving pupils, understanding how this falls within the School's sharing nudes and semi-nudes procedures, and knowing how to respond to and escalate AI-related safeguarding concerns.

11.1.5 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

11.1.6 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in Sharing nudes and semi-nudes: how to respond to an incident (overview) (DfDCMS and UKCIS, March 2024); and Appendix 1 of the School's Safeguarding and Child Protection Policy and Procedures and Searching, screening and confiscation:

advice for schools (DfE, July 2022). In certain cases, it may be appropriate for an authorised member of staff to confiscate the pupil's device to preserve any evidence and hand it to the police for inspection.

11.1.7 All staff are encouraged to adopt and maintain an attitude of 'it could happen here' in relation to sexual violence, sexual harassment and child-on-child abuse and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and/or violent behaviour in the future. It should be made clear there is a zero-tolerance approach to sexual violence and sexual harassment. It is understood that even if there are no reports, it does not mean it is not happening, it may be that it is not being reported.

11.1.8 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.

11.1.9 Staff also receive data protection training on induction and at regular intervals afterwards.

11.1.10 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

11.1.11 Useful online safety resources for staff

a) Safety and Security Online | SWGfL

b) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

c) helpline@saferinternet.org.uk The UK Safer Internet Centre provides an online safety helpline (and email) with expert advice for professionals at 03443814772

d) http://www.childnet.com/teachers-and-professionals

e) Cyberbullying Guidance | Childnet

f) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

g) https://www.thinkuknow.co.uk/teachers/

h) http://educateagainsthate.com/

i) https://www.commonsense.org/education/

j) Preventing Bullying (DfE July 2026)

k) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

l) Sharing nudes and semi-nudes: how to respond to an incident (overview) (DfDCMS and UKCIS, March 2024).

m) Online safety in schools and colleges: questions from the governing board (UKCIS, 2022)

n) Education for a connected world framework (UKCIS, 2020)

o) https://www.lgfl.net/online-safety/resource-centre

p) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

q) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

r) SELMA Hack online hate toolkit (SWGFL, May 2019)

s) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, January 2023)

t) Harmful online challenges and online hoaxes (DfE, February 2021)

u) NSPCC helpline for anyone worried about a child - 0808 800 5000

v) The National Grid for Learning - Safeguarding (lgfl.net)

w) Online safety and schools | NSPCC Learning (NSPCC, September 2024)

x) Home (saferrecruitmentconsortium.org)

y) Internet Watch Foundation If an incident/report involves sexual images or videos that have been shared online, the victim can be supported to get the images removed by the IWF.

z) Report Remove | IWF Childline/IWF's Report Remove is a free tool allowing children to report nude or sexual images and/or videos of themselves that they think might have been shared online.

aa) CEOP Safety Centre The Child Exploitation and Online Protection command is a law enforcement agency working to keep children and young people safe from sexual exploitation and abuse. On their website, online sexual abuse can be reported and a report made to one of its Child Protection Advisors.

bb) Undressed (lgfl.net) LGFL provides schools with advice on how to teach young children about being tricked into getting undressed online in a way that does not scare them or explains the motives of sex offenders.

cc) Safer Internet Filtering and Monitoring Additional filtering and monitoring guidance.

11.1.12 The Royal Borough of Kensington and Chelsea safeguarding children partnership has produced guidance on online safety which is available here: Family Information Hub | Online safety

11.2 Parents

11.2.1 Online safety information and links to resources are provided on the school Parent Portal. These are shown to parents at the September Information Talks. Workshops from outside agencies are held to educate parents on the safe use of technology. The school will take every opportunity to raise parents and carers' awareness of internet safety in communications home. This policy will also be shared on the website with parents and carers.

11.2.2 If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

11.2.3 The school will communicate with parents regarding the filtering and monitoring systems in place, what children are asked to do online (including the websites used) and who (if anyone) from school they will interact with online. Regular governance visits review the effectiveness of filtering and monitoring.

11.2.4 Parents are encouraged to read the acceptable use policy for pupils with their son / daughter to ensure that it is fully understood.

11.2.5 Useful online safety resources for parents

a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

b) http://www.childnet.com/parents-and-carers

c) Parents and Carers Toolkit | Childnet

d) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

e) https://www.thinkuknow.co.uk/parents/

f) http://parentzone.org.uk/

g) https://www.internetmatters.org/resources/

h) https://www.internetmatters.org/

i) https://www.commonsensemedia.org/

j) Advice for parents and carers on cyberbullying (DfE, November 2014).

k) Support for parents and carers to keep children safe online - GOV.UK (www.gov.uk) (DfE, DDCMS, HO, February 2021)

l) http://www.askaboutgames.com

m) https://www.ceop.police.uk/safety-centre

n) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

o) LGfL: parents - scare or prepare

p) Home (lgfl.net)

q) Thinkuknow: what to do if there's a viral scare online

r) I am a parent or carer | How We Can Help | Marie Collins Foundation

s) Stop It Now! UK and Ireland | Preventing child sexual abuse

t) CEOP Education - Protecting children and young people from online child sexual abuse through education (thinkuknow.co.uk)

u) Net Aware update from the NSPCC - UK Safer Internet Centre

v) Talking to your child about online sexual harassment: A guide for parents | Children's Commissioner for England (childrenscommissioner.gov.uk) (Children's Commissioner, December 2021)

w) #AskTheAwkward - help to talk with your children about online relationships (thinkuknow.co.uk)

12 Risk assessment

12.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

12.3 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

12.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to Deputy Head/DSL who has been properly trained in identifying and managing risks.

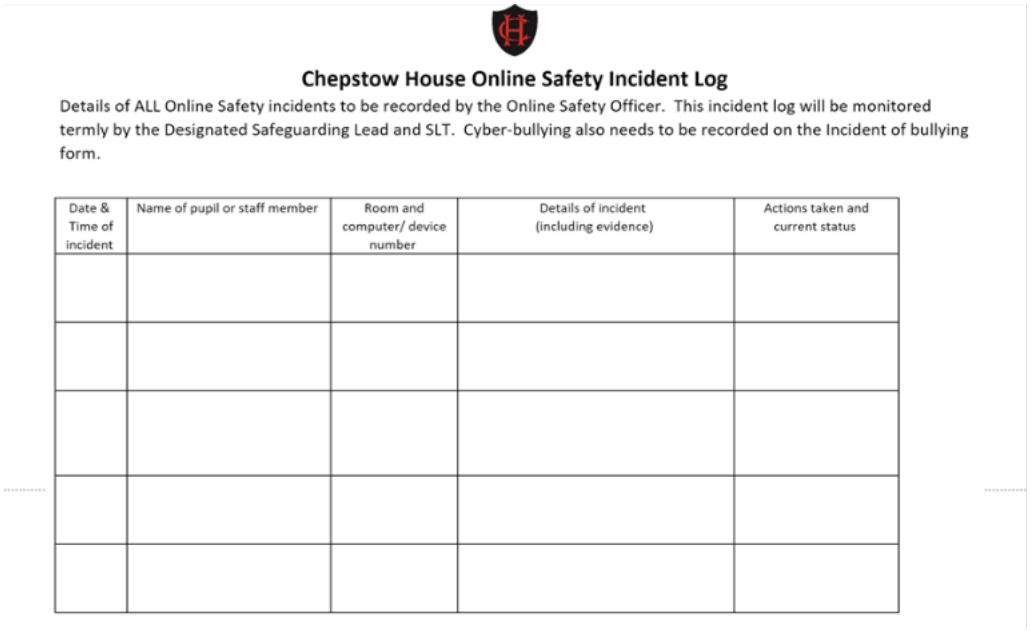
Appendices

Appendix 1

Details of our PSHE Curriculum and Digital Literacy curriculum can be found on our school website. https://www.chepstowhouseschool.co.uk/our-school/educational-philosophy

Appendix 2

Example page from the Online Safety Incident Log.



Chepstow House Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded by the Online Safety Officer. This incident log will be monitored termly by the Designated Safeguarding Lead and SLT. Cyber-bullying also needs to be recorded on the Incident of bullying form.

Date & Time of incident	Name of pupil or staff member	Room and computer/ device number	Details of incident (including evidence)	Actions taken and current status