



Westbourne
House School

CHICHESTER

E-SAFETY POLICY

This is the policy of Westbourne House School, which incorporates the Prep School, Pre-Prep, Early Years Foundation Stage as well as provision for boarding

Policy Statement

This policy applies to all members of the school (including pupils, staff, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the School. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers. In due regard to E-Safety throughout the school, we also comply with Keeping Children Safe in Education (KCSIE) 2025 and its attendant guidance specifically: [Online safety \(e-safety\) and schools | NSPCC Learning](#).

In due regard to E-Safety, we aim to safeguard the pupils and staff. Both this policy and the Acceptable Use Agreements (which pupils complete electronically during their ICT lessons at the beginning of each school year) 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 and watches etc). To safeguard children and practitioners online, it is helpful to refer to the guidance in 'Safeguarding children and protecting professionals in early years settings: online safety considerations' (<https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations>)

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. This will be carried out by the governors receiving information about e-safety incidents and monitoring reports on an annual basis.

Headmaster:

- The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Head of ICT.
- The Headmaster and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse”).

Head of ICT:

- Leads the E-safety Committee which is part of the ICT Development Committee.
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. Making sure they keep up-to-date on current e-safety guidance.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets, when necessary, with the Governors to discuss current issues.
- Reports, when necessary, to Senior Management Team

Network Manager:

- Ensures that the School's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensures that users may only access the networks and devices through enforced password protection.
- Ensures that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role, and to inform and update others as relevant.
- Ensures that the use of the network, internet, intranet, remote access, email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headmaster and Head of ICT for investigation/action/sanction.

Teaching and Support Staff:

- Must have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.
- Must have read, understood and signed the Staff Acceptable Use Policy (SAUP).
- Reports any suspected misuse or problem to the Headmaster/Senior Management Team or Head of ICT for investigation/action/sanction.
- Ensures all digital communications with pupils/parents/carers is on a professional level *and only carried out using official school systems.*
- Ensures that pupils understand and follow the acceptable use policies.
- Ensures that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Designated Safeguarding Lead (DSL):

Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming

- Cyber-bullying
- And to have due regard for the monitoring and filtering systems that are in place.

The DSL is expected to review the filtering and monitoring provision at least annually as set out in KCSIE 2025 with routine monitoring taking place on a regular basis.

The responsibility of those named above (Network Manager, Head of ICT and the DSL and to include the SMT) should ensure that the filtering system is sufficiently robust to block harmful and inappropriate content without unreasonably impacting teaching and learning. See also [Appropriate Filtering and Monitoring - UK Safer Internet Centre](#)

(NB: It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop).

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters and the School's website and information about national/local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website.
- Their children's personal devices in the school (where this is allowed).

Education and Training

Pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need

the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of ICT/Learning for Life and is regularly revisited.
- Key e-safety messages can be reinforced as part of assemblies and pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 Anti-Bullying and Cyber-Bullying Policy).
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. *(The School has enhanced software to assist in this e.g, Veyon: [Veyon | Cross-platform computer control and classroom management](#)).*

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography (*see AI and 'deep fake' below) fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying); and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

In addition to the above this policy takes into consider recent KCSIE inclusion (under online harms): disinformation (*false information deliberately created and spread to mislead others, cause harm, or for political/economic gain*) misinformation (*false or inaccurate information spread unintentionally*) and conspiracy theories (*which intersect with the 4 'C's above and can manifest under all 4 'C's largely as misinformation*).

NB: *The School recognises the safeguarding risks arising from Artificial Intelligence (AI), including the manipulation or misuse of images (e.g. deepfakes).

Staff must report any suspected misuse of pupil images involving AI. The School prohibits the use of AI systems for processing pupil images, other than through approved suppliers under contract who meet our safeguarding and data protection standards.

Parents/carers:

Parents and carers safety risks play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The School will therefore seek to provide information and awareness to parents and carers through:

- Newsletters or the School website
- Parents/Carers sessions
- High profile events e.g., Safer Internet Day
- Reference to the relevant web sites/publications:
 - www.swgfl.org.uk
 - www.saferinternet.org.uk
 - www.childnet.com/parents-and-carers
 - www.thinkuknow.co.uk
 - www.commonsemmedia.com
 - [Staying safe online - West Sussex County Council](#)

Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training is made available to staff. This will be regularly updated and reinforced. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school's E-Safety policy and Acceptable Use Agreements.
- The Head of ICT will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.

- The Head of ICT will provide advice/guidance/training to individuals as required.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (or Head of ICT) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Governors:

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by relevant organisations.
- Participation in school training/information sessions for staff or parents

Policy Statements

Infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- All users will have clearly defined access rights to school technical systems and devices.
- All users (at Year 3 and above) will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school's ICT system, used by the Network Manager, must also be available to the Headmaster and kept in a secure place.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. There is a clear process in place to deal with requests for filtering changes.
- The School has provided enhanced/differentiated user-level filtering e.g., Smoothwall: [Smoothwall | Education | Digital Safeguarding Solutions](#)
- School technical staff monitor and record the activity of users on the school technical systems when necessary.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed (see Appendices for reporting log).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that staff and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of School and Personal Devices

Staff

Refer to the Employee Handbook for further guidance on the use of non-school owned electronic devices for work purposes.

- School devices which are 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 a device is not in use, staff should ensure that it is locked to prevent unauthorised access.
- Staff are permitted to bring in personal devices for their own use.

Pupils

Refer to the BYOD Policy for further guidance.

- As a rule, pupils are not allowed to bring mobile phones into School ([*Mobile phones in schools Guidance for schools on prohibiting the use of mobile phones throughout the school day February 2024*](#)). For the few that have permission e.g., those that come to school using a bike, that pupil bring must hand their mobile phone into Reception at the start of the day and then it may be collected when they leave School. These requirements apply to phones, tablets and Smart Watches. It is very unlikely that a Smart Watch would ever be required, similarly a tablet and, again, as a rule of thumb, these devices are not allowed at School. Laptops for those children that have permission to use them are looked after by the IN Department.
- The School recognises that personal 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 Individual Needs department to agree how the School can appropriately support such use. The Individual Needs Department will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at School.
- Before such a device can be used the pupil will need to read and sign the school Pupil BYOD Policy and ask a member of the IT department to set up the relevant access on the device.

- Our International and full-time boarders are allowed devices in school for communicating with family and friends. These devices are not accessible to the children outside of set and supervised times and are set up using the School's filtering and monitoring systems.

Communications

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

- Staff must not access social networking sites, any website or personal email which is unconnected with school work or business whilst teaching / in front of pupils.
- Training to include: acceptable use, social media risks, checking of settings, data protection, and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- No reference should be made in social media to pupils, parents/carers or school staff without prior permission.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff should not make contact with pupils, should not accept or initiate friend requests nor follow pupils via social media.
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications can be monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, 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.
- Any digital communication between staff and pupils or parents/carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

The following table outlines what the school considers is appropriate use of communication technology for staff, other adults and pupils:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected pupils	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phone in lessons		X						
Use of mobile phone in social times	X						X	
Taking photos on mobile phones / personal cameras				X				
Use of other mobile devices eg: tablets, gaming devices		X					X	
Use of personal email addresses in school, or on school network		X					X	
Use of school emails for personal emails				X	X			
Use of messaging apps		X					X	
Use of social media		X					X	
Use of blogs			X			X		

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 cyber-bullying 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 images on the internet e.g. on social networking sites.

- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Parents or carers provide permission to the school regarding the use of photos within the Terms and Conditions that they sign upon their child entering the school.
- The School recognises the safeguarding risks arising from Artificial Intelligence (AI), including the manipulation or misuse of images (e.g. deepfakes). Staff must report any suspected misuse of pupil images involving AI. (See above: Education & Training)

Data Storage and Processing (Please refer to the Data Protection Policy for further details)

- Staff and pupils are expected to save all data relating to their work to their school laptop or the school's central server.
- The school expects all removable media (USB memory sticks etc) taken off the school site to be encrypted.
- 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.
- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT should be immediately reported to the Network Manager or Head of ICT.

Misuse

Some internet activity (e.g. accessing child abuse images) is illegal. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context.

In the event of suspicion, it is important that all of the following steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to

these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national/local organisation (as relevant)
 - Police involvement and/or action
- If content being reviewed includes images of Child Abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

The school adopts a zero-tolerance approach to any cyber bullying issues, all staff will challenge any abusive behaviour between peers that comes to their notice and will report on to the DSL immediately any issues of this nature. Please see the Child Protection (Safeguarding) Policy for further details about dealing with peer-on-peer abuse.

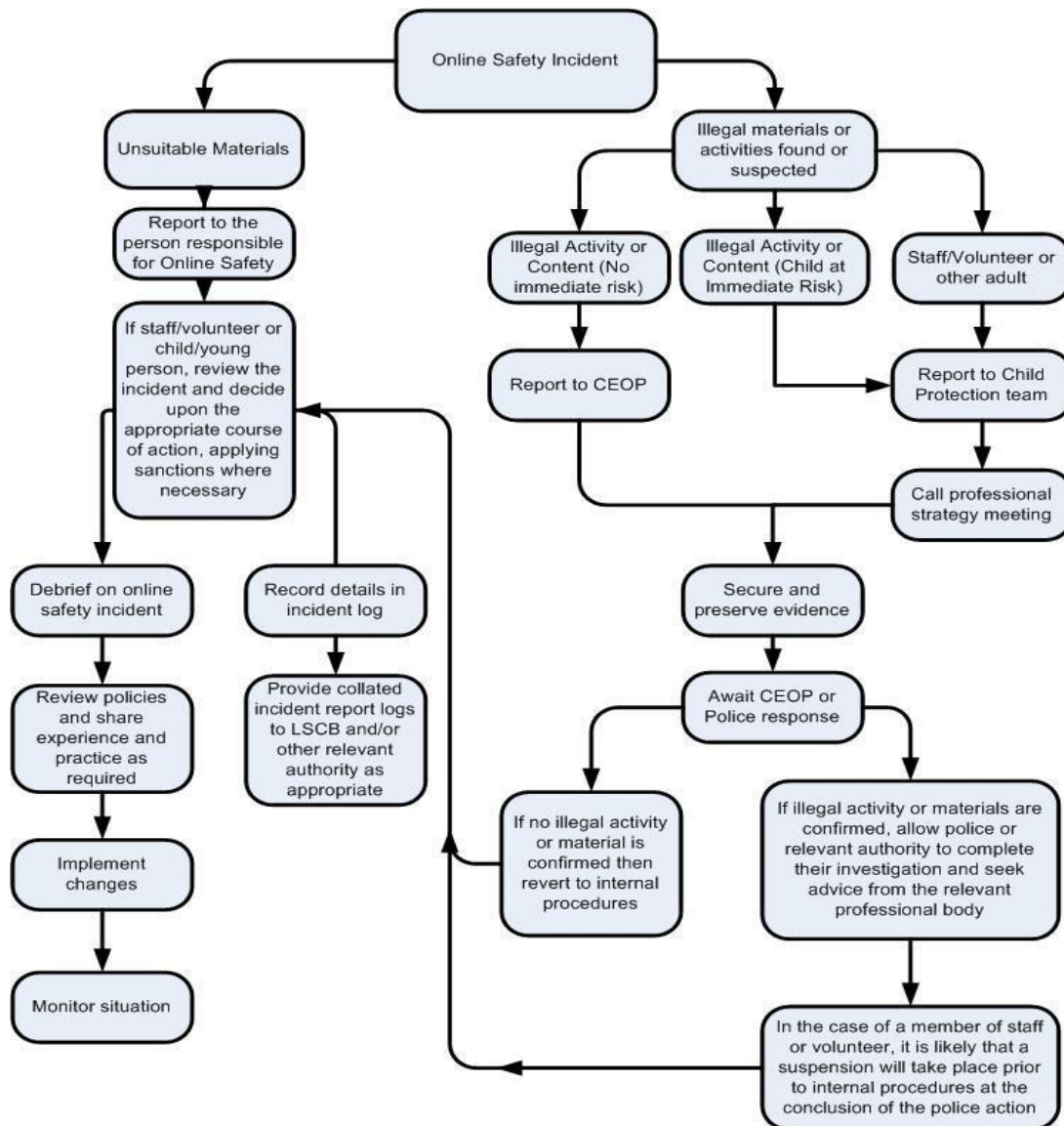
The school believes that the activities referred to in the following table would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational)	X					
On-line gaming (non educational)		X				
On-line gambling				X		
On-line shopping / commerce		X				
File sharing		X				
Use of social media		X				

Use of messaging apps		X			
Use of video broadcasting eg YouTube		X			

The following flowchart outlines the procedure to follow after any member of the community perceives there to have been an online safety incident.



School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that

incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Department / Head of Year/DSL	Refer to Headmaster	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device		X					X		X
Unauthorised use of social media / messaging apps / personal email		X			X				
Unauthorised downloading or uploading of files		X							
Allowing others to access school network by sharing username and passwords		X						X	
Attempting to access or accessing the school network, using another student's / pupil's account		X					X		X
Attempting to access or accessing the school network, using the account of a member of staff		X	X			X	X		X

Corrupting or destroying the data of other users		X							X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		X	
Continued infringements of the above, following previous warnings or sanctions			X				X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			X
Using proxy sites or other means to subvert the school's filtering system		X			X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			X	
Deliberately accessing or trying to access offensive or pornographic material		X							X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X	

Staff	Actions / Sanctions
--------------	----------------------------

Incidents:	Refer to line manager	Refer to Headmaster (and or DSL)	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			
Inappropriate personal use of the internet / social media / personal email						X	
Unauthorised downloading or uploading of files						X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X					
Careless use of personal data eg holding or transferring data in an insecure manner	X						
Deliberate actions to breach data protection or network security rules	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software							X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X	
Actions which could compromise the staff member's professional standing		X				X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X	
Using proxy sites or other means to subvert the school's filtering system	X					X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X	
Deliberately accessing or trying to access offensive or pornographic material		X	X				X
Breaching copyright or licensing regulations	X						
Continued infringements of the above, following previous warnings or sanctions		X	X				X

Acknowledgements

South West Grid for Learning
ISBA

Monitoring and review

The School will review and monitor the effectiveness and compliance of this policy (and appendices – if appropriate). This policy will be kept up-to-date and amended to take account of legislative and regulatory changes.

Last Review Date	Next Review Date	Reviewer(s)
September 2025	September 2026	Head of ICT Head of Pre-Prep Designated Safeguarding Lead

Acceptable Use of School Devices Agreement for pupils in Years 1-4

*Pre-Prep pupils read as a class; the class teacher keeps a copy displayed in the classroom.
Year 3 and 4 pupils sign an individual copy*

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer
- I will not share images of pupils or staff to Artificial Intelligence (AI) platforms unless this is part of an approved school system and with prior authorisation.

I have read and understood the above and agree to follow the guidelines:

Name of Pupil:

Signed:

Date:

Acceptable Use of School Devices Agreement for pupils in Years 5-8

I understand that I must use the school ICT systems and equipment in a responsible way, to ensure that there is no risk to my safety and security of the ICT systems, equipment and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger' when I am communicating on-line.
- I will immediately report any unpleasant or inappropriate material, messages or anything that makes me feel uncomfortable when I see it on-line.

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

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

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions to my own.
- I will not take or distribute images of anyone without their permission.
- I will only use my own personal devices in school if I have permission. I understand that, if I do use my own device in school, I will follow the rules set out in the Bring Your Own Device (BYOD) Policy and User Agreement.
- I understand the risks and will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others. Nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email.
- I will not install, attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school but involved in the membership of the school community (e.g. on a school trip).
- I understand that if I fail to comply with this Acceptable Use of School Devices Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules in this Agreement.

I have read and understood the above and agree to follow the guidelines:

Name of Pupil:

Signed :

Date:

Acceptable Use of School Devices Agreement for Parents/Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.
- Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name:

Pupil Name:

As the parent / carer of the above-named pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Year 3 - 8

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

Pre-Prep

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

Signed

Date

Acceptable Use of School Devices Agreement for Staff & Volunteers

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:



Westbourne
House School
CHICHESTER

School Training Needs Audit

Name	Position	Relevant Training in last 12 months	Identified Training Needs	To be met by	Cost	Review Date