Colegio Hispano Británico

Líder mundial en enseñanzas británicas

Online Safety Policy

Policy Creation and Review	
Author(s)	Angela Nudds
Last Review Date	August 2023 Angela Nudds
Next Review Date	August 2024

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of Colegio Hispano Británico. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Colegio Hispano Británico will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

<u>Roles and Responsibilities</u>

The following section outlines the online safety roles and responsibilities of individuals and groups within Colegio Hispano Británico:

Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about online safety incidents and monitoring reports. A member of the Directors will take on the role of Online Safety Person. The role of the Online Safety Person will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- reporting to relevant Directors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Person.
- The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety person and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Person.

Online Safety Officer / Person

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with the Directors to discuss current issues,
- attends relevant meetings
- reports regularly to Senior Leadership Team

Network Support

The Technical Team and Co-ordinator for Computing are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, learning platforms, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Online Safety Person for investigation
- that monitoring software is implemented and updated in line with Keeping children safe in Education (2019).

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher, Senior Leadership Team, Online Safety Person for investigation.
- they report any data breach or suspected data breach to the Online Safety Person without delay

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Child Protection Leads

Should be trained in Online 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
- online-bullying

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online 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 in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and the website. Information about national and local online safety campaigns will be promoted via Twitter and, if necessary, via email. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- Theirs and their children's personal devices when used in school

Policy Statements

Education – 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 digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- key online safety messages should be reinforced as part of a planned programme of Worships and classroom activities
- pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's online behaviours. Parents may underestimate how often children and young people 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:

- Curriculum activities
- Letters, newsletters, web site, social media
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to relevant web sites and publications

Education & Training – Staff / Volunteers

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

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Person and other members of staff as appropriate will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Person will provide advice and training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 online safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

There will be regular reviews and audits of the safety and security of school

Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school's technical systems and devices.
- All users will be provided with a username and secure password by the Computing Coordinator 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 Computing Coordinator, alongside external service providers, is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses 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. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Computing Coordinator will regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (see Data Protection Policy) 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.

Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's cloud based services such as SSuite, email and data storage.

All users should understand that the primary purpose of the use of mobile and/or personal devices in a school context is educational.

- The school's Acceptable Use Agreements for staff, pupils and parents / carers will give consideration to the use of mobile technologies

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes (only for those pupils who walk/bus to & from school alone)*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet access	Yes	Yes	Yes	No	Yes	*Upon request*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

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.

- written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media, school prospectus, newsletter, internal displays
- in accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published and/or 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 school policies 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.

- 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.
- Pupils' full names will not be used anywhere on a website, blog and social media, particularly in association with photographs.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permssion	
Mobile phones may be brought to the school				✓		✓		
Use of mobile phones in lessons				✓				
Use of mobile phones in social time				✓				
Taking photos on school mobile phones / cameras		✓						
Use of other mobile devices e.g. tablets						✓	✓	
Use of personal email addresses in school or on school network		✓	✓	✓				
Use of school email for personal emails		✓	✓		✓ (with restrictions)			
Use of messaging apps	✓			✓				

Use of social media		✓		✓				
Use of blogs	✓				✓			

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are 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, social media, chat, blogs, 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.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online 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.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School / academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- 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

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school.
- The school will effectively respond to social media comments made by others according to a defined policy or process

Dealing with unsuitable / inappropriate activities

Colegio Hispano Britanico believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in and/or outside the school. The school policy restricts usage as follows:

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– 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	
	Promotion of extremism or terrorism				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 e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies and will understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- 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 – see below)
- 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 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
    - promotion of terrorism or extremism
    - 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.**

It is important that all of the above 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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 procedures as follows:

Students / Pupils Incidents	Refer to class teacher/Computing Coordinator	Refer to Head of Key Stage	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. 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	X		X
Unauthorised use of non-educational sites during lessons	X		X	X	X		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X	X	X		
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X	X	X		
Unauthorised downloading or uploading of files	X	X	X	X	X		

Allowing others to access school network by sharing username and passwords	X		X	X	X		X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	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	X	X		X	
Students / Pupils Incidents	Refer	Refer to Head of Key Stage	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. exclusion
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	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	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X		X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X	X	

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	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	X	X
Inappropriate personal use of the internet / social media / personal email		X	X		X	X	X
Unauthorised downloading or uploading of files		X	X		X	X	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 e.g. holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X	X			X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X			X	X	X

Actions which could compromise the staff member's professional standing		X			X	X	X
Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X			X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system		X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X
Breaching copyright or licensing regulations		X		X	X		
Continued infringements of the above, following previous warnings or sanctions		X					X