Cañada Blanch Spanish School
Founded 1972

E-SAFETY POLICY including EYFS

This is a whole school policy

Revised: January 2020
Ratified by the Headteacher and Safeguarding Lead
Review Date: January 2021

Instituto Español Vicente Cañada Blanch
317 Portobello Road
London W10 5SZ
Tel: 020 8969 2664
canada.blanch.uk@educacion.gob.es
http://vicentecanadablanch.educalab.es/home

Overview

Aims

This policy aims to:

- Set out expectations for all community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline) at the Instituto Español Vicente Cañada Blanch.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare students for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the students in their care.
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Code of Conduct or Anti-Bullying Policy)

Scope

This policy applies to all members of the Instituto Español Vicente Cañada Blanch community (including staff, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

I.E.Vicente Cañada Blanch is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

Headteacher/Principal – María del Carmen Pinilla Padilla

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the Designated Safeguarding Lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.
- Liaise with the Designated Safeguarding Lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling, helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.
- Ensure that there is a system in place to monitor and support the ICT Team who carry out internal technical online-safety procedures.

Designated Safeguarding Lead - María del Mar Brea Ruiz

Key responsibilities:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure there is regular review and open communication between the school and the ICT Team.
- Ensure "An effective approach to online safety that empowers the school to protect and educate the community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children".
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.

- Work with the headteacher to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safety.
- Review and update this policy, other online safety documents and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the proprietors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Liaise with school technical and support staff as appropriate.
- Communicate regularly with SLT and the designated ICT Team to discuss current issues review incident logs and filtering/change control logs and discuss how filtering and monitoring.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - cascade knowledge of risks and opportunities throughout the organisation

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know That the Designated Safeguarding Lead (DSL) is Mar Brea, the ICT Manager is Fernando Ramos and the ICT Coordinators are Antonio Simon, Lucia Buceta and Cristina Salmeron.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education.
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle, so do not keep anything to yourself.
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL/ICT Team if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.

- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Whenever overseeing the use of technology in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and data law.
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL/ICT Team of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues in the playground, corridors, and other communal areas outside the classroom – let the DSL/ICT Team know.
- Model safe, responsible and professional behaviours in their own use of technology.

IT Manager/technician Fernando Ramos/Joaquín Rodríguez

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead and the ICT Team to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems, especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL, ICT Team and SLT. Currently, our network is protected with 3 filters:
  The **Basic filter** is a simple protection against malware, advertisements and basic security.
  While the **Protected filter**, in addition to basic protection, acts as a barrier to adult websites, gambling sites, download sites, unsecured addresses and other websites unsuitable for minors. This is the filter we use at all times.
  The **Custom filter** is a web filter in which you can specify specific web addresses. It is usually only used for public computers and/or exceptional cases.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.

Volunteers and contractors

Key responsibilities:

- Read and understand this policy.
- Report any concerns, no matter how small, to the Designated Safeguarding Lead / ICT Team.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Pupils

Key responsibilities:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/carers

Key responsibilities:

- Read and understand this policy and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, proprietors, contractors, pupils or other parents/carers.

Handling online-safety concerns and incidents

Online safety concerns must be handled in the same way as any other safeguarding concern, so all professionals should err on the side of talking to designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies :

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Code of Conduct

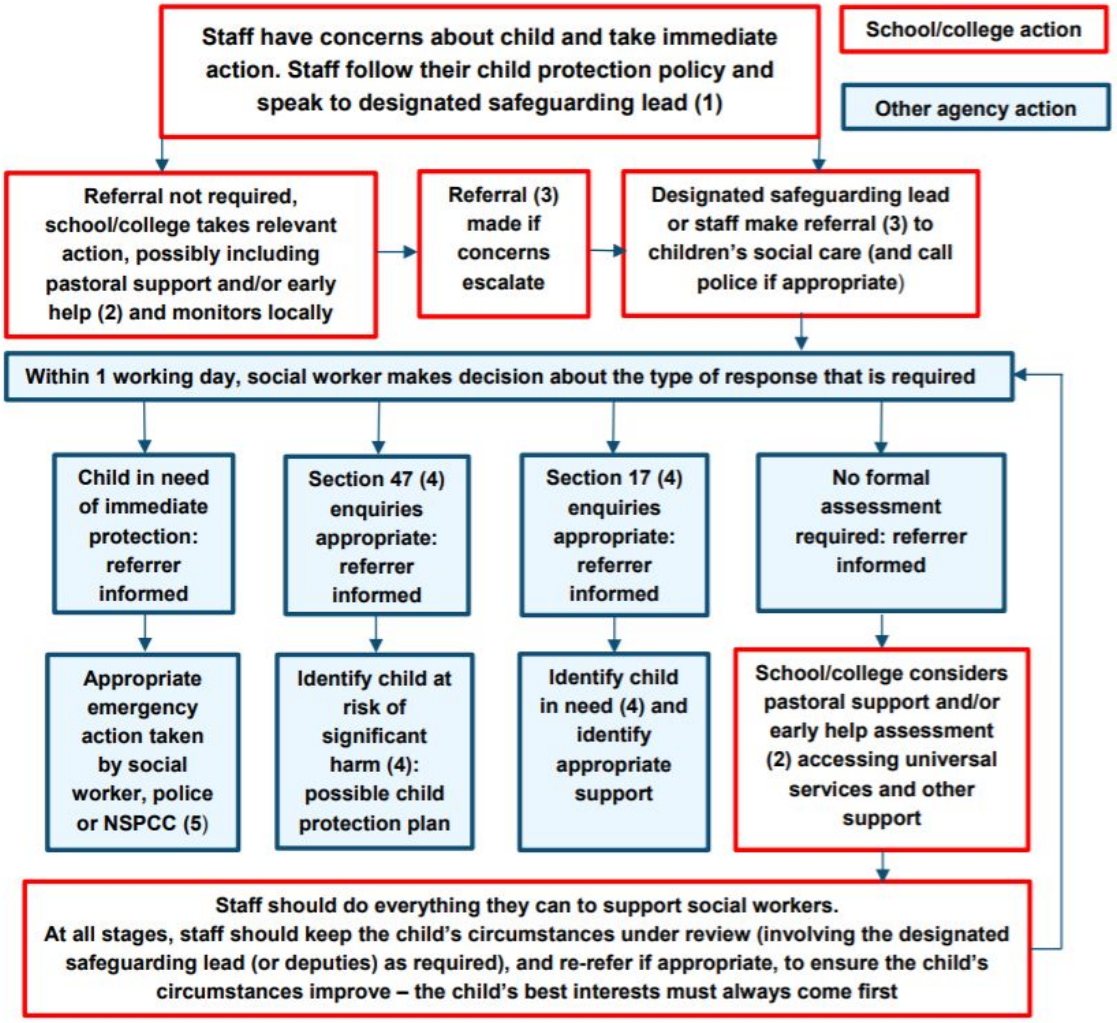
I.E. Vicente Cañada Blanch commits to take all reasonable precautions to ensure online safety, but recognises that incidents may occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the ICT Team / Designated Safeguarding Lead on the same day.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to Consejería de Educación and the LADO (Local Authorities Designated Officer).

Actions where there are concerns about a child

page 16 of Keeping Children Safe in Education 2019 as the key education safeguarding document.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Check the Instituto Español Vicente Cañada Blanch website for the Anti-bullying policy for more information.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The school takes all forms of sexual violence and harassment seriously, explains how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and are not allowed to perpetuate.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media.

Where pupils contravene these rules, the school Code of Conduct will be applied. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Data protection and data security

The headteacher and the DSL work together to ensure the UK's implementation of the General Data Protection Regulation, or GDPR for storing data, which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material and children can be taught with regards to online teaching and safeguarding.

At I.E. Vicente Cañada Blanch, the internet connection is provided just for teachers. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and security, including a web filtering system, which is made specifically to protect children in schools. All our computers have a freezing protection program that restores all settings to the original configuration after shutting down the computer, which is done automatically at 8:00 pm every day

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom and public and private spaces at the school, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Electronic communications

Please read this section alongside references to pupil-staff communications in the school Code of Conduct This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

School website

The school website is a key public-facing information portal for the school community with a key reputational value. The Headteacher has delegated the day-to-day responsibility of updating the content of the website to the ICT Coordinators and the ICT Manager

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Instituto Español Vicente Cañada, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing. Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social media

SM presence of the Instituto Español Vicente Cañada

The Instituto Español Vicente Cañada works on the principle that if we don't manage our social media reputation, someone else will. Accordingly, we manage and monitor our social media footprint

carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Designated teachers are responsible for managing our School Blog and Twitter. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document.

Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. We expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school, which is important for the pupils we serve.

The school has an official Twitter account and will respond to general enquiries about the school, but asks parents/carers not to use this channel to communicate about their children. Email is the only accepted electronic communication channel between parents and the school, and between staff and pupils.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices and bring your own device (BYOD) policy

- **Pupils/students** are allowed to bring mobile phones, however they are not allowed to use them in any case/scenario unless the teacher has given express permission as part of a lesson. Any attempt to use a phone in lessons or elsewhere within the school premises without permission or to take illicit photographs or videos will lead to disciplinary actions. Important messages and phone calls to or from parents should be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children (including EYFS teachers)**, should leave their mobile phones on silent and only use them in private staff areas during school hours.
- **Volunteers, contractors,** should leave their mobile phones on silent and only use them in private staff areas during school hours. Under no circumstances should they be used in the presence of children or to take photographs or videos.

Network / internet access on school devices

- **Pupils/students** are not allowed to access the school wireless internet. However, they are allowed to use their own internet in their personal devices for school-related activities and when the teacher has specified so. All such use is monitored.
- **All staff who work directly with children (including EYFS teachers)**, should leave their mobile phones on silent and only use them in private staff areas during school hours.
- **Volunteers, contractors, proprietors** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.

Trips / events away from school

For school trips/events away from school, teachers will use their personal phone, ensuring that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

The Headteacher and staff are authorised and have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendices

CONSENTIMIENTO PARENTAL

Bajo el Reglamento General de Protección de Datos de la UE (GDPR) se requiere el consentimiento explícito para comunicarse con las familias.

COMUNICACIÓN

Autorizo que la escuela me contacte vía:

	SI	NO
Teléfono		
Correo electrónico		
Mensaje de texto		

ACTIVIDADES EXTRAESCOLARES

Autorizo que mi hijo tome parte:

	SI	NO
En eventos supervisados en sitios cercanos a la escuela		

USO DE IMAGEN E INFORMACIÓN (incluyendo fotos y videos)

Autorizo a mis hijos:

	SI	NO
Su imagen sea usada para exposiciones/ murales/actividades de clase		
Imagen, sin nombre, para ser publicada en web oficial de la escuela, cuenta de twitter		
Trabajos con nombre para ser exhibidos en la escuela en exposiciones		

Podrá retirar su consentimiento en cualquier momento contactando con la escuela.

Londres a ..... de ..... de 20.....

Fdo.: .....