Prior Park College

E-SAFETY POLICY
Prior Park College

Policy Owner Assistant Head Well Being	**Applies to** Prior Park College (PPC)	**Superseded documents** E-Safety Policy v2
Associated documents Safeguarding Policy The Prevent Duty Policy *See section 14 for the full list of associated policies*	**Review frequency** Every year (unless the legislation/regulations update before this time) **Implementation date** September 2022	**Legal Framework** KCSIE 2022 The Prevent Duty Relationship Education, Relationship and Sex Education and Health Education Equality Act 2010

This policy is reviewed annually, or more regularly as required, prior to approval by Trustees, where applicable.

Last reviewed by:	Assistant Head Wellbeing (Mr Dave Sackett) and Head of Compliance (Miss Emma Wickham)
Date last reviewed:	August 2022
Approved by Trustees:	NA Approved by SLT
Date last approved:	29 September 2022
Date for next approval:	September 2023

1. Introduction

Prior Park Schools (PPS) is a family of Christian schools based in Bath and Gibraltar. Prior Park College (PPC) and The Paragon School (TP) are incorporated in England as Prior Park Educational Trust Ltd. Prior Park School Gibraltar (PPSG), is incorporated in Gibraltar as Prior Park School Ltd. Both are companies limited by guarantee and registered charities.

The Prior Park Schools mission, underpinned by shared values, is to steward a thriving family of communities with love for the young people they serve at their heart. These vibrant communities cultivate creativity, foster integrity, and transform lives.

Prior Park Schools Values:
Curiosity – Generosity – Courage

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile devices')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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, such as 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, involvement in illegal and/or immoral hacking activities

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

4. Definition

E-Safety: E- safety (Electronic safety) is often referred to as online safety, internet safety and/or web safety. E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, gaming devices, email etc). In practice, e-safety is as much about behaviour as it is electronic security.

Staff: Throughout this policy the term 'staff' refers to staff, Trustees, other volunteers, visitors, agency staff and contractors.

VPN: Virtual Private Network. It makes your browsing private, hides your IP (Internet Protocol) address and ensures your internet service provider (ISP) doesn't track you.

Securly: The internet filtering and monitoring software in place across all PLDs. It filters appropriately to year group age and alters the E-Safety Lead and DSL if a student's search includes a disturbing key word from a defined list.

PLD: Personal Learning Device – devices provided and maintained by the school

NSD: Non School Device (including laptops, phones, smart watches, iPads) – devices not provided and maintained by the school.

DSL: Designated Safeguarding Lead

DDSL: Deputy Designated Safeguarding Lead

5. Roles and responsibilities

The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The Board of trustees will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding lead (DSL).

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Head

The Head is responsible for ensuring that all staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and Deputy DSLs are set out in our Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, with the support of the DDSL with responsibility for E-Safety (Assistant Head Well Being) in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school safeguarding policy
- Ensuring that any online safety incidents are logged (on CPOMs, where applicable) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Anti-Bullying Policy and Behaviour Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head and/or Board of Trustees as applicable/required

This list is not intended to be exhaustive.

E-Safety Lead (DDSL)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the School online safety policies and documents.
- 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.
- Works with the tutor and HsM on any student concerns.
- Works with the Peer Mentors to deliver student support.
- Liaises with the Local Authority / relevant body, where appropriate.
- Liaises with School technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Attends any Trustee meetings or SLT meetings and reports regularly to Senior Leadership Team.
- Promotes an awareness and commitment to e-safeguarding throughout the School

Community.

- Ensures that e-safety education is embedded across the curriculum.
- To communicate regularly with SLT and Trustees to discuss current issues, review incident logs and filtering / change control logs.
- To ensure that an e-safety incident log is kept up to date.
- To feedback on concerns, trends and students of concern to the DSL and DDSL's in the half termly safeguarding meeting.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and are passed onto the DDSL/DSL to be dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are passed on to the DDSL/DSL to be dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use.
- Working with the DSL/DDSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Anti-Bullying Policy and Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Students are expected to:

- Read, understand and agreed to the terms on acceptable use of the school's ICT systems and internet
- Keep their logon details secure
- Report any concerns to a member of staff

Parents are expected to:

- Notify a member of staff or the Deputy Head Pastoral (DSL) of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Interporternet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

Reporting Harmful Content on Social Media Platforms – reportharmfulcontent.com

Visitors

Visitors who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

6. Educating students about online safety

Students will be taught about online safety as part of the curriculum. Delivery is principally through the PSHCE programme, and this is further supported in the teaching of ICT and through pastoral activities and assemblies.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **time a student leaves PPC** we will ensure they know and understand:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- To understand that any use of online communication (including that on social media, gaming platforms and messaging services) impacts on their digital footprint, which future employers may discover
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and students with SEND.

7. Educating parents about online safety

The school will raise parents' awareness of internet safety in communications to home, and as part of regular information evenings. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Deputy Head Pastoral (DSL).

Concerns or queries about this policy can be raised with the Deputy Head Pastoral (DSL).

8. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-Bullying Policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Conversations around cyberbullying are woven into the PSHCE curriculum from the very first year of study and is revisited in each year.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes other subjects and pastoral settings where appropriate.

All staff, Trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

The Head, Deputy Head Pastoral (and DSL), Deputy Head Academic, Deputy DSL's, HsMs and House Parents can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will immediately inform the DSL (or DDSL).

When deciding if there is an exceptional reason to erase data or files from a device, the DSL will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the **DSL (or DDSL) immediately**, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Conducting a Student Search Policy
- Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

9. Acceptable use of the internet in school

All students, parents, staff, volunteers and trustees must sign a digital agreement before being given access the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

During the school day, use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Boarding House students will have access to the school's internet, in the evening and at weekends, for personal and non-educational purposes, though all access will remain monitored and filtered as appropriate.

We will filter the websites visited by students to ensure they comply with the above. This is via Securly, the College's monitoring and filtering software.

10. Students using mobile devices in school

Students may bring mobile devices into school, but they should remain 'invisible' and are not permitted to use them during:

- Lessons* (except for the Personal Learning Device (PLD) approved by PPC- see the Mobile Device Policy for more information)
- Travelling between lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- In the dining hall

**There may be occasions when students completing computer science are required to use NSD's, this will be agreed and approved by SLT beforehand.*

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the Behaviour Policy, which may result in the confiscation of their device.

11. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse children online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

13. Monitoring arrangements

The DSL/DDSLs review online safety in the termly safeguarding meeting.

This policy will be reviewed every year by the Assistant Head Wellbeing. At every review, the policy will be shared with the DSL, Head and Local Board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Safeguarding Policy
- The Prevent Duty Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Privacy Notice(s)
- Complaints Policy
- Anti-Bullying Policy
- Mobile Device Policy
- Social Media Policy
- Taking, Storing and Using Images Policy
- Acceptable Use of ICT Services for staff

Appendix A: Student E-Safety Acceptable Use of IT Services Agreement

As a student at one of the Prior Park Schools you will need to access a wide variety of IT services to support your studies and your life in the school community. These services may be accessed on school or personal devices, on the school site or remotely. This document details how we expect you to use these services as a responsible member of the school.

Definitions

- The term "personal learning device" (**PLD**) refers to all school issued computing devices.
- The term "non-school device" (**NSD**) refers to any personal electronic device, not issued by the school. This includes all non-school-issued mobile phones, smartphones, laptops or tablets, smart watches and emerging technologies.
- The term "mobile devices" includes both PLDs and NSDs.

Acceptable Use (How we expect you to use the school IT services)

Central to the effective use of the PLDs in school are the following 3 principles which state that you must:

- Use the PLD for approved educational activities only
- Treat the PLD assigned to you and those assigned to others with respect
- Not install or attempt to install any hardware or software without the permission of the school

It is expressly forbidden for any student to use mobile devices for any of the following purposes:

- To bully and harass another student or member of staff
- To take photographs and recordings (video and audio) in class, a house, changing room or any other space in the school without the express permission of a specific teacher (who takes responsibility for that action)
- To carry out any activities which are against either the principles or details of the School Behaviour Policy
- To access, download or circulate inappropriate materials, e.g. pornography, racist/hateful content, extremist propaganda
- To cheat in examinations or plagiarise academic work
- To affect any form of communication that brings the school into disrepute or defames groups or individuals
- To upload or share images, video and other content that is indecent or could embarrass or harass others or could break the law
- To game, chat or engage in other distracting behaviours during lesson or activity time, without the express permission of the supervising teacher
- To try to install non-approved software, attempt to get around any school security or safeguarding system or to attempt to physically open the PLD and tamper with the hardware or affect any aspect of the start-up procedure.
- To pick keys off the keyboard, scratch or deface the casing, prise off any of the rubber feet or screen spacers or physically alter the PLD in any way.

It is expected that all students will:

- Follow this agreement at all times and the associated polices; E-Safety Policy, Behaviour Policy and Anti-Bullying Policy

- Always use a carry case when transporting the PLD inside and outside of school
- Take reasonable care to prevent damage to the PLD and will not cause any malicious damage, graffiti, or use stickers on a PLD
- Comply with the ICT system security and not disclose any passwords, to anyone else, provided to them by the school or other related authorities
- Not connect to open public Wi-Fi hotspots
- Not attempt to circumvent school security systems via the use of Virtual Private Networks or by any other means
- Be held responsible for all activity carried out under their username and while the PLD is assigned to them
- Ensure that all data is kept secure and is used in accordance with school policies both in school and off-site. If students are unsure, they should seek clarification
- Not browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory, or pornographic
- Report any issues with the devices to the ICT support staff as soon as is reasonably practical
- Use the device for educational purposes, only as directed by their teachers in lessons and prep periods
- Understand that all online activity using the PLD is logged and monitored both inside and outside school and that school safeguarding staff may be automatically alerted to any concerning behaviour
- Understand that on-screen activity whilst using a PLD during school time can be readily viewed by a teacher, school leader, or appropriate member of support staff to promote positive behaviour for learning, for safeguarding or child protection, or for other educational purposes
- Understand and accept that appropriate staff members reserve the right to block internet access as deemed necessary to enhance teaching and learning
- Only use the PLD assigned to them
- Understand the primary educational purpose of the PLDs, either at home or in school, and that their behaviour and use of the device must reflect this

PLD Damage

Accidents happen - if the PLD suffers accidental damage then this will be repaired free-of-charge for the first incident. Any further accidental damage that occurs during this academic year may be charged. As soon as the PLD has an accident, bring it to the IT office for assessment and repair. You will be given a temporary PLD whilst repairs are carried out.

If however, it is clear to the IT team that the damage is deliberate or as a result of careless neglect then there will be a charge for repair or replacement.

By signing this electronically, you are confirming that you have read, understood and agree to the above expected behaviours and acceptable use of the IT system and services.

Name of Student:

Signature of Student:

Date: