E-SAFETY POLICY
The Paragon School

Policy Owner Deputy Head Pastoral and DSL	**Applies to** The Paragon School	**Superseded documents** PPS E-Safety Policy v1
Associated documents All TPS specific and PPS Associated Safeguarding Policies	**Review frequency** Every year (unless the legislation/regulations update before this time) **Implementation date** 19 January 2024	**Legal Framework** KCSIE 2023 Working Together 2018 Prevent 2015

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

Last reviewed by:	Deputy Head Pastoral & DSL (Mrs Sarah James)
Date last reviewed:	September 2023
Approved by Trustees:	The Paragon School SLT
Date last approved:	10 January 2024
Date for next approval:	January 2025

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

At The Paragon we recognise the duty to safeguard the welfare of children: protecting them from maltreatment; preventing impairment of children's health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care and taking action to enable all children to have the best possible outcome. All staff have a role to play in safeguarding children. The Paragon will work with all relevant agencies to promote the welfare of children and protect them from harm as a fundamental part of our intent to provide excellent pastoral care to all pupils.

The E-Safety Policy should be read in conjunction with the TP Safeguarding Policy.

All action is taken in line with relevant legislation and guidance including:

- Keeping Children Safe in Education (DFE Sept 2023) [Sexual Violence and Sexual Harassment between children in schools and colleges Sept 2021 which has been subsumed into KCSIE 2022]
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (2020)
- What to do if you are worried a child is being abused (March 2015)
- Working Together to Safeguard Children (2018)
- Revised Prevent Duty Guidance for England & Wales (April 2019)
- The Prevent Duty: departmental advice for schools (June 2015)
- The use of social media for online radicalisation (July 2015)
- Relationship's education, relationships and sex education (RSE) and health education (July 2019)
- EYFS Statutory Framework 2021
- NSPCC; When to call the Police
- The Children Act 1989, The Children Act 2004
- Education Act 2002, Section 175 and Section 157
- Independent School Standards Regulations November 2014
- South West Child Protection Procedures (SWCPP) at www.swcpp.org.uk
- Bath & North East Somerset Community Safety and Safeguarding Partnership

Additional guidance is also provided by UK Council for Child Internet safety (UKCCIS) and NSPCC.

E-safety is the process of limiting risks to children and young people when using Information and Communications Technology (ICT). E-safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT- fixed or mobile; current, emerging and future ICT.

The Paragon prides itself on its innovative approach to the use of technology in line with its ethos and aims. All teaching staff and pupils in Years 5 and 6 are given a PLD (Personal Learning Device) to support and enhance their learning, supported by a powerful infrastructure including excellent Wifi, cloud storage and interactive boards in every classroom. The school is eager for pupils to make the most of the opportunities afforded by the use of technology but does so with the safeguarding of every child's welfare at the heart of every decision.

2. Definitions

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

3. Policy Statement

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to online safety.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all trustees, staff, volunteers, children and young people and anyone involved in The Paragon's activities.

4. Policy Aims

At The Paragon we believe that:

- children and young people should never experience abuse of any kind,
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

At The Paragon we recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges.
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- we have a responsibility to help keep children and young people safe online, whether or not they are using Prior Park Schools' network and devices.
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.
- working in partnership with children, young people, their parents, guardians and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- a member of the Leadership Team takes on responsibility as E-Safety Coordinator/Online Safety Lead.
- providing clear and specific directions to staff and volunteers on how to behave online through our Staff Code of Conduct Policy.
- supporting and encouraging the pupils to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- supporting and encouraging parents and guardians to do what they can to keep their children safe online.
- developing an online safety agreement for use with pupils and their parents/guardians.
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a pupil.
- reviewing and updating the security, filtering and monitoring of our information systems regularly.
- ensuring that usernames, logins, email accounts and passwords are used effectively.
- ensuring personal information about staff and pupils who are involved in our organisation is held securely and shared only as appropriate, in line with our Data Protection Policy.
- ensuring that images of pupils are used only after their (or their parents') written consent has been obtained, and only for the purpose for which consent has been given.
- providing supervision, support and training for staff and volunteers about online safety.
- examining and risk assessing any social media platforms and new technologies before they are used within the school.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse – see Safeguarding Policy for more information (including online abuse),
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation,
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account,
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

5. E-Safety Risks & Issues

What is E-Safety?

E-Safety is a term that encompasses not only the internet, but all other ways in which young people communicate using electronic media (e.g. smart phone, gaming consoles). It means ensuring that young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves and others.

E-safety risks and issues can be roughly classified into four areas: content, contact, conduct and commerce. The following are basic examples of the types of e-safety risk and issues that could fall under each category.

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts - Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice
Commerce (child as consumer)	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks	phishing and financial scam	Sextortion, trafficking for purposes or sexual exploitation, streaming child sexual abuse	Information filtering, profiling bias, polarisation, persuasive design

6. 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

7. 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 pupils 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,
- Will ensure that the filtering and monitoring systems used fully protect children when online.

The Head

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

The Designated Safeguarding Lead

Details of the school's DSL and DDSL's are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, 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, the 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 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 schools Positive 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 headteacher and/or governing board,
- Ensure that staff are trained and aware of their filtering and monitoring responsibilities and what to do if they are concerned about something a child has accessed online.

This list is not intended to be exhaustive.

The E-Safety Coordinator/Online Safety Lead

The E-Safety Coordinator, Online Safety Lead (OSL), is a member of the Leadership Team, and is responsible for:

- 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.
- Liaises with the Local Authority / relevant body.
- Liaises with School technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Attends LT meetings when asked and reports regularly to Senior Leadership Team when applicable.
- 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 DSL 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.
- Ensures the filtering and monitoring systems used by the school are working and providing relevant information to support the school in keeping children safe online.

This list is not intended to be exhaustive.

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 pupils 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files in liaison with the DSL and E-Safety lead.
- 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 schools Positive Behaviour Policy.
- Works closely with the DSL to ensure that the children's online activities are safe and appropriate.

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 pupils follow the school's terms on acceptable use.
- Working with the DSL 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 schools Positive Behaviour Policy and Anti-Bullying 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.

Pupils

- When they reach Year 5&6 and start to have more freedom of their own Personal Learning Device, are responsible for using the School digital technology systems in accordance with the Pupil Acceptable ICT Use Agreement (Appendix A).
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff, DSL or the Head of any concerns or queries regarding this policy.
- When their child starts to use a school PLD in Years 5&6, ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix A)
- When their child is in Year 5&6, ensure they have read, understood and agreed to the terms on their child's acceptable use of the school's ICT systems and internet and reinforce this at home as well.

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

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community 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.

8. Educating pupils about online safety

The Paragon is a member of National Online Safety. This service aids staff and parents with resources and training required to deliver a safe online environment for the young people at the school.

Staff: awareness and training

- New staff receive information on The Paragon's E-Safety and IT use policies as part of their induction by the DSL.
- All staff receive regular information and training on E-safety issues in the form of Safeguarding INSET training, either in person on via EduCare and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-safety. All supply staff and contractors receive information about e-Safety as part of their safeguarding briefing on arrival at school.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School E-Safety procedures. These behaviours are summarised in the pupil acceptable use policy which must be signed and returned before use of technologies in School. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines. They re-sign the document at the start of each academic year.
- All staff should be monitoring any usage of computers and be aware of what children in their class are accessing, or trying to access so support can be given.

Teaching staff are expected to incorporate E-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff on CPOMs as soon as possible if any incident relating to E-safety occurs, which will notify the School's DSL and DDSLs (E-safety co-ordinator).

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, as well as their role in the filtering and monitoring of online activity.

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 their peers 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.
- How the school filters and monitors the online activities of children and their role in supporting this.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence pupils 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.

Pupils: E-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for E-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote E-safety and regularly monitor and assess our pupils' understanding of it.

To support the pupils in embodying the five Paragon Values when online as well as remaining safe, the school encourages the children to be SMART online:

Safe
Meeting
Ask
Reliable
Tell

The School provides opportunities to teach about E-safety within a range of curriculum areas and Computing lessons. Educating pupils on the dangers of technologies that may be encountered

outside School will also be carried out via Personal Development, by presentations in assemblies, as well as informally when opportunities arise.
At age-appropriate levels, usually via Personal Development, pupils are taught about their E-safety responsibilities and to look at their own online safety. Pupils can report concerns to the DSL, the DDSL any member of staff at the school.

From Year 3, pupils are also gradually taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

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 the School's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach any member of staff as well as parents, or peers for advice or help if they experience problems when using the internet and related technologies.

Teaching staff access to teaching resources, lesson plans and CPD via The National Online Safety to support the delivery of e-safety in our curriculum.

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

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Parents

- The School seeks to work closely with parents and guardians in promoting a culture of e-safety.

- The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.
- The School recognises that not all parents and guardians may feel equipped to protect their child(ren) when they use electronic equipment at home.
- The School therefore arranges regular entries surrounding e-safety in the weekly bulletin.

9. 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 pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, 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 pupils, 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 pupils, 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 can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, 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 of an electronic device, the authorised staff member will:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff.
- Explain to the pupil why we feel it is necessary to look at what is on their electronic device how it will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation.
- Depending on the risk identified, staff may contact parents before they search a device.

Staff members, who have been authorised to do so by the Director of Operations and Finance, 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 pupil 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 a pupils electronic device 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 Pupil Search Policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

10. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of 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.

The 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.

We will monitor the websites visited by pupils, staff, volunteers, Trustees and visitors (where relevant) to ensure they comply with the above.

Further information is available for staff on the Staff Portal.

11. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. Monitoring arrangements – Filtering and monitoring

The Paragon School understands the risks associated with children accessing uncensored material online. Therefore, the school has different levels of filtering and monitoring in place for school devices and on the school network to ensure the safety of our children when online. The parameters of the filtering and monitoring block harmful and inappropriate content without unreasonably impacting teaching and learning.

These are:

☺ Cisco Meraki - the school's network system has content filtering in place which has been
set up to ensure children are not able to access, via the internet in school, inappropriate content.

☺ Bitdefender – this has been installed on all school owned devices and is an end point security system that protects against virus/malware threats that could expose children's data, as well as providing a further layer of content filtering.

☺ Securly – this filtering and monitoring system monitors the low-level detail of what the children are typing and accessing and ensures that children are not able to access uncensored web content. Securly will inform the safeguarding and IT teams of any attempt to access inappropriate content so that it can be followed up. Additionally, it will log any concerning activity for the safeguarding team to follow up with the child.

All staff are responsible for:

- monitoring the usage of devices and the contact children are accessing. Staff should show their professional curiosity when children are online by looking at their screens and supporting their web searches.
- Teaching children about responsible digital behaviour, ethics and the consequences of inappropriate online actions.
- Report if witness or suspect unsuitable material has been accessed or notice abbreviations or misspellings that allow access to restricted materials.

The DSL is responsible for monitoring any safeguarding concerns which are flagged by staff or by the system and following them up in an appropriate way.

The ICT team are responsible for ensuring that the different levels of security are operating effectively. The team will review the filtering and monitoring at least annually and ensure that it is sufficient to meet the changing needs of the children and the internet. The IT team will work with the DSL to ensure the children are safe.

The Safeguarding Trustee is responsible for ensuring that the school is fulfilling their responsibilities in this area.

The DSL/DDSL logs behaviour and safeguarding issues related to online safety in the Blocked Usage Log (Appendix B) and where applicable via CPOMs.

This policy will be reviewed every year by the Deputy Head Pastoral (DSL) and DDSL with responsibility for E-Safety. At every review, the policy will be shared with the Local Board of Trustees.

13. Links with other policies

This online safety policy is linked to our:

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

APPENDIX A- Acceptable Use Policy and Agreement

The Paragon Acceptable use policy for Personal Learning Devices (Y5 and Y6 pupils).

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. They 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.

In order to use the school's PLDs, I will agree to the following:

- I will keep my passwords for login into my Personal Learning Device (PLD) or application to myself – if I think others know my passwords, I will tell my teacher.
- I will only use my PLD for activities related to school.
- I shall use the online activities and sites which school allows me to access from home
- appropriately.
- I will only use my PLD to access material related to my schoolwork.
- Any messages I send will be polite and respectful in line with the Paragon Values.
- I will always report anything that I feel is unkind or makes me feel unsafe or
- uncomfortable to my teacher or other adult. I will not reply to any nasty messages.
- I will always keep my personal details private (e.g. my name, mobile phone number,
- family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without permission.
- I will not share files or photos without permission.
- I will not share any photos of myself, or my friends, in our school uniform.
- I understand that the school will check my computer files and will monitor the
- Internet sites I visit.
- I will treat my PLD like all school equipment; with care and respect, using the case provided.
- I know that I am responsible for ensuring that my PLD is in school, and I manage the battery level so that I can use it in lessons each day.
- I know that if I break this agreement, I might not be allowed to use my PLD.

Signed:

Name:

Date:

Parent / Carer

As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my son /daughter as part of whole school commitment to e-Safety 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. I understand that my child'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.

Name of Pupil:
Class:

Signed (parent/carer):

Name:

Date:

APPENDIX B Blocked Usage Log Template

Date	Child	Year Group	Alert	Action