ONLINE SAFETY POLICY

Prior Park Paragon

Policy Owner Deputy Head Pastoral and DSL	**Applies to** Prior Park Paragon	**Superseded documents** TP_E-Safety Policy v3
Associated documents All PPP specific and PPS Associated Safeguarding Policies	**Review frequency** Every year (unless the legislation/regulations update before this time) **Implementation date** 2 September 2026	**Legal Framework** KCSIE 2026 Working Together to Safeguard Children 2026 Data Protection Act 2018 Data (Use and Access) Act 2025 The Early Years Foundation Stage: Statutory Framework September 2026 Crime and Policing Act 2026 Online Act 2023

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 S James) and Head of Compliance (Miss E Wickham)
Date last reviewed:	August 2026
Approved by Trustees:	Approved by Senior Leadership Team
Date last approved:	1 September 2026
Date for next approval:	September 2027

1. Introduction

Prior Park Schools (PPS) is a family of Christian schools based in Bath and Gibraltar. Prior Park College (PPC) and Prior Park Paragon (PPP) are incorporated in England as Prior Park Educational Trust Ltd. Prior Park Gibraltar (PPG), 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 Prior Park 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. Prior Park 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 Online Safety Policy should be read in conjunction with the PPP Safeguarding Policy.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 phones')
- 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user 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; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation and guidance

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

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education (RSE) and health education – remove if not applicable, see section 4]
- 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.

4. Roles and responsibilities

4.1 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Trustees will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Board of Trustees will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Board of Trustees will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All Trustees will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

4.2 The Head

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

4.3 The designated safeguarding lead (DSL)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head and Trustees to review this policy and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing Trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the Head of IT to make sure the appropriate systems and processes are in place
- Working with the Head, Head of IT 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school 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
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

4.4 The Head of IT

The Head of IT is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's IT 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 IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are reported, logged and dealt with appropriately in line with this policy and PPP Safeguarding Policy
- Making sure that any incidents of cyber-bullying are reported dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.5 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 IT systems and the internet, and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL and Head of IT
- Following the correct procedures of completing a request for service ticket on the staff portal if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school 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.

4.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Make sure that, where relevant, their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

4.7 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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating Pupils About Online Safety

5.1 Pupils will be taught about online safety as part of the curriculum

Prior Park Paragon educates pupils about online safety through Personal Development and Computing lessons. The subject is also covered in whole school initiatives, whole school assemblies and Key Stage assemblies. This service aids staff and parents with resources and training required to deliver a safe online environment for the young people at the school.

IT and online resources are used increasingly across the curriculum. We believe it is essential for Online-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.

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this

- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with 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 some pupils with SEND.

For more information about how this area is specifically taught at Prior Park Paragon through Computing and Personal Development lessons, refer to the relevant schemes of work.

5.2 Pupils will be taught practical cyber security skills
The following items come from the DfE's non-statutory cyber security standards for schools and colleges.
All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

6. Educating parents about Online Safety

The school will raise parents/carers' awareness of relevant internet safety through our bulletin or other communications home, and in information via our website. This policy will also be shared with parents/carers via our website.

We will also invite outside speakers into school to educate parents about topics to do with Online Safety, as well as share how we support this in school.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the DSL or the Head.

7. Cyberbullying

7.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Positive Behaviour Policy.)

7.2 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 encourage them 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. Class teachers will discuss cyber-bullying with their classes during PD lessons, Computing lessons and also during specific weeks such as 'Anti-Bullying Week' and 'Internet Safety Week'.

All staff, Trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and anti-bullying 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

The Head or DSL, 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, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from other agencies
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, 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 DSL and/or Head 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 first consider the appropriate safeguarding response. Refer to PPP Safeguarding Policy for further information.

When deciding whether there is a good reason to erase data or files from a device, staff members 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/carer 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 equivalent) 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 pupils 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
- PPS Conducting a Student 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.

7.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Prior Park Paragon recognises that AI has many uses but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

At Prior Park Paragon, during the school day pupil use of AI is not allowed. However, we do teach children about AI though our Computing and PD curriculum, as well as during events such as 'Safer Internet Week'.

Prior Park Schools will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying and Positive Behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should seek advice from the Head of IT and Head of Compliance before using any form of AI which is not pre-approved as per the AI for Staff Policy.

8. Acceptable use of Internet at Prior Park Paragon

Pupils (when given their PLD in Year 6), staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

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 and restrict access through filtering systems where appropriate.

9. Pupils using mobile devices in school

Prior Park Paragon is a mobile free school, and pupils are not permitted to bring mobile devices to school.

On occasion, pupils who walk to school, or for other reasons, may need to bring their mobile device for safety reasons. In this instance, parents are asked to read and comply with our PPP Mobile Phone (children) Policy. In this instance, the child's mobile phone is handed into the reception desk when they arrive and collected as they leave.

Any breach of this policy, for example a child having aphone on them during the school day, may trigger disciplinary action in line with the schools Positive Behaviour Policy and their device may be confiscated.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring all anti-virus and anti-spyware software is updated when required
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use. More information can be found in PPS Remote Working Policy and the Acceptable Use of IT Policy.

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 acceptable use. 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 PPS Disciplinary Process and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training for all staff, Trustees and volunteers

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 their peers online through:
    - Abusive, threatening, 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLand DDSLs 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 child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the DSL and HOC.

At every review, the policy will be shared with the Board of Trustees, and all staff will be asked to read it and assure the DSL that they have understood their responsibilities within the policy.

14. Filtering and monitoring

Prior Park Paragon 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.

☺ SENSO – this enables staff to monitor the online activity of each child in real-time and enables them to support each child with content as they are online.

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 IT 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 Trustees are responsible for ensuring that the school is fulfilling their responsibilities in this area. This is discussed during the termly Safeguarding Meetings with the Trustee responsible for Safeguarding, DSL and HOC.

The DSL logs behaviour and safeguarding issues related to online safety in the Blocked Usage Log and where applicable via CPOMs.

APPENDIX A- Acceptable Use Policy and Agreement

Prior Park Paragon Acceptable use Policy for Personal Learning Devices (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 Prior Park 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: