Perryfields Enterprise Academy Trust

Online Safety Policy

Adapted From:	The Key model policy
Reviewed:	October 2026
Approved By:	Trust Board
Approved Date:	15th October 2026
Review:	Annually
Next Review Date:	October 2027
Communicated to Staff	By: Email Date:
Published on:	PJS website

SUMMARY OF CHANGES – September 2026	
Section	**Detail**
	New Policy

Contents

1. Aims 3
2. Legislation and guidance 4
3. Roles and responsibilities 4
4. Educating pupils about online safety 7
5. Educating parents/carers about online safety 9
6. Cyber-bullying 9
7. Acceptable use of the internet in school 11
8. Pupils using mobile devices in school 12
9. Bring Your Own Device and Personal Devices 12
10. Social media 13
11. Staff using devices outside school 13
12. How the school will respond to misuse 14
13. Training for staff, governors and volunteers 14
14. Monitoring arrangements ..... **Error! Bookmark not defined.**
15. Links with other policies ..... **Error! Bookmark not defined.**
Appendix 1: KS2 Acceptable Use Policy for Pupils ..... **Error! Bookmark not defined.**
Appendix 2: KS2 Acceptable Use Policy for Parents/Carers 16
Appendix 3: Acceptable Use Policy for Staff, Governors and Volunteers 21
Appendix 4: Acceptable Use Policy for Visitors and Contractors 24
Appendix 5: online safety incident report log 24

---

1. 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

Scope of this Policy:
This policy applies to all members of the school community, including pupils, staff, volunteers, governors, parents/carers, visitors and community users who access or use the school's ICT systems, whether on or off site.

The school recognises that online safety incidents may occur both within and outside the school environment. In accordance with the Education and Inspections Act 2006 and the Education Act 2011, the school may take action where online behaviour has an impact on the welfare, safety or reputation of the school community.

The school will work with parents/carers and external agencies, where appropriate, in relation to incidents that occur outside school but are linked to members of the school community.

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

2. 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
- 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. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governing board 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

The governor who oversees online safety is **Joanna Clarke.**

All governors will:

- Make sure 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 (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college 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

3.2 The headteacher

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

The headteacher will:

- Ensure there are effective arrangements for monitoring and supporting staff undertaking online safety responsibilities.
- Ensure appropriate filtering and monitoring reports are reviewed regularly.
- Ensure staff receive appropriate online safety training.
- Be aware of procedures to be followed in the event of a safeguarding or online safety allegation involving a member of staff.
- Ensure online safety forms part of the whole-school safeguarding approach.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) 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:

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school

- Review this policy annually 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 governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the Teaching, Learning and Digital Lead to make sure the appropriate systems and processes are in place
- Working with Teaching, Learning and Digital Lead 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 (see appendix 5) 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
- 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.

3.4 The Teaching, Learning and Digital Lead

The Teaching, Learning and Digital Lead 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) 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
- Liaising regularly with the DSL regarding online safety matters
- Providing advice and guidance to staff
- Monitoring the effectiveness of filtering and monitoring systems
- Supporting staff in the safe use of online technologies and remote learning platforms

This list is not intended to be exhaustive.

3.5 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
- Maintaining an up-to-date awareness of online safety issues and emerging risks
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), 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
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) 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'
- Promoting online safety across the curriculum where appropriate.
- Supporting pupils in developing 'critical thinking', safe research practices and respect for copyright
- Using only authorised school communication systems when communicating with pupils and parents/carers
- Reporting any concerns regarding filtering, monitoring or inappropriate content immediately
- Monitoring pupil use of digital technology during lessons and school activities

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that 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

3.7 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 (appendix 4).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

- Relationships and sex education and health education in secondary schools

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.

4.2 Pupils will be taught practical cyber security skills

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.

4.3 Radicalisation and Extremism

Pupils will be taught about the risks associated with online radicalisation, extremism, misinformation and harmful influence.

The school recognises that extremist groups may use online platforms to target vulnerable individuals and will include age-appropriate education to help pupils:

- Recognise harmful online content
- Critically evaluate information
- Understand how online influence and manipulation may occur
- Know how and where to seek support

Education relating to the Prevent Duty forms part of the school's wider safeguarding curriculum.

5. Educating parents/carers about online safety

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Teaching, Learning and Digital Lead.

Parents/carers may also be directed to external support organisations including Childnet, Internet Matters, Parent Zone, UK Safer Internet Centre, CEOP and Childline resources.

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

6. Cyber-bullying

6.1 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 behaviour policy.)

6.2 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 class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors 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).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, 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 the headteacher
- 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 the staff member in conjunction with the DSL / headteacher 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.

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
- Our behaviour and relationships 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.

6.4 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.

The governing board recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others, facilitate harassment, spread misinformation, misuse a person's identify or create inappropriate content. 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.

The governing board will treat any use of AI to bully pupils, harass others, create inappropriate images, spread harmful content or otherwise cause harm very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI Policy.

Any misuse of AI technologies by pupils or staff will be addressed through the appropriate safeguarding, behaviour, disciplinary or staff conduct procedures, as applicable.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 4.

7.1 Remote education and live streaming

The school recognises the importance of maintaining appropriate safeguarding arrangements when technology is used to support remote education, online learning and live-streamed activities.

Staff and pupils must adhere to the requirements set out in this Online Safety Policy when participating in remote learning activities.

Further guidance regarding the safe delivery of remote education, staff expectations, pupil participation and safeguarding arrangements can be found in the school's Remote Learning Policy, which should be read alongside this policy.

7.2 Digital images and videos

Staff and pupils must use digital images and video recordings responsibly.

The school will:

- Obtain appropriate permissions before publishing pupil images
- Ensure images are used only for authorised educational or promotional purposes
- Educate pupils about the risks associated with sharing images online
- Ensure staff follow school procedures regarding the creation, storage and sharing of images.

The sharing of inappropriate images, including nude or semi-nude images will be addressed through the school's safeguarding procedures.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are required to leave them turned off and at the school office throughout the school day and they may collect them when leaving.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's behaviour policy, which may result in the confiscation of their device.

9. Bring Your Own Device (BYOD) and Personal Devices

The school recognises that personal devices may be used in connection with school activities where authorised. The use of personal devices must not compromise safeguarding, data protection, network security or the learning environment.

All staff, pupils, governors, volunteers and visitors using personal devices in connection with school activities must comply with this Online Safety Policy and the school's acceptable use requirements.

Further guidance on the use of personal devices, including permitted use, responsibilities, security requirements and monitoring arrangements, can be found in the school's Bring Your Own Device (BYOD) Policy, which should be read alongside this policy.

10. Social media

The school recognises the importance of responsible social media use in protecting pupils, staff and the wider school community.

Guidance relating to personal use of social media is contained within the school's Social Media Policy, which should be ready alongside this policy.

11. 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 – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- 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, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Teaching, Learning and Digital Lead

12. 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 and internet acceptable use. 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 addressed in accordance with the Staff Code of Conduct and disciplinary procedures.

All incidents will be investigated proportionately, documented appropriately and managed according to the nature, seriousness and circumstances of the incident.

Where appropriate, the school may:

- Preserve evidence
- Restrict access to systems, accounts or devices
- Involve parents/carers
- Consult external agencies
- Refer matters to children's social care or the police.

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

Any suspected illegal content, including child sexual abuse material, will be referred immediately to the police and managed in accordance with statutory safeguarding guidance.

Online safety incidents will be logged and monitored by the DSL and Teaching, Learning and Digital Lead to identify trends emerging risks and any further actions required to safeguard pupils and staff.

In addition to incidents occurring within school, the school may respond to online safety concerns that occur outside where the behaviour affects the wellbeing, safety or reputation of members of the school community.

All actions taken will be proportionate, reasonable and in line with the school's safeguarding, behaviour, disciplinary and complaints procedures.

13. Training for staff, governors 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 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.

Governors 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.

14. Monitoring arrangements

The DSL will ensure that online safety incidents, behaviour concerns and safeguarding issues relating to the use of technology are appropriately recorded, monitored and reviewed. An incident report log can be found in appendix 5.

The effectiveness and impact of this policy will be monitored through:

- Online safety incident logs
- Safeguarding records
- Filtering and monitoring reports
- Feedback from pupils, staff and parents/carers, where appropriate
- Annual reviews of online safety risks, emerging technologies and safeguarding trends

Information gathered through these monitoring activities will be used to inform staff training, curriculum development, safeguarding practice and any required updates to the school's online safety arrangements.

This policy will be reviewed annually by the Teaching, Learning and Digital Lead to ensure that it remains effective, up to date and compliant with current legislation, statutory guidance and best practice. Any significant online safety incident, change in legislation, statutory guidance or emerging risk may require an earlier review. Following every review, this policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

- Acceptable Use Policies
- Behaviour and Relationships Policy

- Bring Your Own Device Policy
- Child Protection Policy
- Cyber Security Policy
- Data Protection Policy
- Discipline and Dismissal Procedure
- Mobile Phones Policy
- Remote Learning Policy
- Social Media Policy
- Staff Code of Conduct
- Teaching and Learning Policy
- Use of Artificial Intelligence Policy

16. Appendix 1: KS2 Acceptable Use Policy for Pupils

LGfL SafeguardED

Acceptable Use Policy (AUP) for KS2 PUPILS

My Online Safety Rules (KS2)

Being Safe

- **I will follow the school rules:** I will use school devices and the internet only when I am allowed and for schoolwork.
- **I keep passwords safe:** I will never share my passwords and will tell a teacher if someone else finds them out.
- **I check before I click:** I will not click on strange links that I do not know, or pop-ups without checking with a teacher, or parent/carer, nor download things without permission.
- **I respect age limits:** I will not use 13+ games or apps, as they are not safe for me.
- **I protect my identity:** I will not share private details like my address or phone number.
- **I can say no online if I need to:** I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I will say no, stop chatting and tell a trusted adult immediately.
- **I am a safe researcher**: I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across.
- **I don't livestream on my own**: I check with a trusted adult before I video chat with anybody for the first time.

Being Kind

- **I am a good friend and ally:** I will not post or share unkind, rude, or hurtful messages, images, or videos. If a friend is worried or needs help, I remind them to talk to an adult, report it, or even do it for them.
- **I know what 'banter' means:** I know that calling someone names is not 'fun' or 'banter'—it can hurt people.
- **I don't take secret photos or videos:** I will not take pictures or videos of others without their permission. I will never create fake images, videos, or 'deepfakes' of anyone.
- **I respect work:** I only use other people's work (pictures or words) if I have permission.

Using Technology Responsibly

- **I check with an adult:** I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. I will talk to a trusted adult before chatting with anyone new, even if they claim to be a friend or are a 'chatbot'.
- **I know my body is mine:** I will not send photos or videos of myself or get changed in front of a camera. If I feel uncomfortable, I will stop and tell a trusted adult.
- **I don't pretend to be someone else:** I am always honest about who I am online.
- **I am careful what I share and protect my online reputation:** I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

LGfL SafeguardED

Acceptable Use Policy (AUP) for KS2 PUPILS

What to do if something goes wrong

- **It's not my fault:** If I see something bad online or receive an unkind message, it is **not** my fault. I will not get in trouble for telling an adult.
- **I tell someone:** If I see or experience something that makes me feel worried, upset, or confused, I will stop what I am doing and tell a trusted adult straight away.

My Trusted Adults

At school, my trusted adults are: **teachers, LSAs, midday assistants or admin staff.**

At home, my trusted adult/s is/are: _____

I know I can also get in touch with Childline at 0800 1111

Signed: _____ **Date:** _____

17. Appendix 2: KS2 Acceptable Use Policy for Parents/Carers

LGfL SafeguardED

Acceptable Use Policy (AUP) for PARENTS/CARERS

INTRODUCTION & BACKGROUND

Technology is an essential part of daily life and learning. At Perryfields Junior School your child's safety and wellbeing are our utmost priority. We expect pupils to act with equal respect and care whether they are online or face-to-face, inside or outside of school.

We ask parents and carers to sign this policy to help reinforce these safe behaviours. Your child has signed a matching age-appropriate AUP. Our full Online Safety Policy can be found at [https://www.perryfields-jun.essex.sch.uk/page/school-policies/137246]. If you have any questions, please contact our Designated Safeguarding Lead (DSL) (Mrs Edwards or our Digital and Online Safety Lead (Miss Kingston).

Perryfields Junior School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children in our care for their future lives. We take every reasonable precaution to keep pupils safe online as outlined in the government's guidance.

1. DEVICES IN SCHOOL

- **Filtering & Monitoring:** I understand the school uses filtering (website blocking) and monitoring to protect pupils. While school network protections are safer than most home networks, no system is 100% risk-free. The school aims to teach safe and responsible use, rather than 'overblocking' educational content.
- **Mobile Phones & Personal Devices:** I will support the school's policy regarding personal devices brought to school. I will not call or text my child during the school day; urgent messages must always go through the school office.
- **Tracking Devices:** I will not attempt to track my child during the school day or on school trips using Apple AirTags or similar devices. Doing so violates product terms, can broadcast locations to strangers, and causes unnecessary distress during routine route adjustments.
- **School Communications:** Staff will only contact my child regarding learning or wellbeing through approved systems as outlined in the school's Remote Learning Policy. I will report any unusual or external app contact requests immediately to the DSL (Mrs Edwards).

2. AT HOME & REMOTE LEARNING

- **Filtering:** I understand that any school-owned devices and cloud platforms that are used out of school are subject to filtering and monitoring. More detail of this can be found in our online safety policy.
- **Safe Environment:** I will help my child maintain safe habits at home and during remote learning.
- **Video Call Etiquette:** During school video calls, I will ensure my child is fully dressed (not in bed) and that their camera points away from personal spaces or uses a blurred background.
- **Private Online Tutors:** If I arrange private online tuition, I will verify their safety credentials using the *Online Tutors – Keeping Children Safe* guidelines and ensure sessions happen in a shared family room.
- **Home Protections & Boundaries:** I will utilise parental controls, home filtering, and child-safe search tools like swiggle.org.uk or YouTube Kids. I will promote a healthy balance using the *Digital 5 A Day* framework. Parental guidance is available at parentsafe.lgfl.net.
- **Regular Dialogue:** To help understand what my child does online and ensure they are confident to talk to me should something go wrong, I will regularly talk to my child about their life online. Parental guidance is available at parentsafe.lgfl.net.

3. IN THE COMMUNITY & SOCIAL MEDIA

- **Modelling Digital Respect:** I will model safe, positive online behaviours. I will refrain from sharing images or details without permission or posting negative, threatening, or abusive comments about school staff, governors, pupils, or other parents on social media. The school will request the prompt deletion of abusive posts and contact the police if an offence occurs.
- **Age Restrictions & Group Chats:** The impact of social media use is often felt strongly in schools. I will support age restrictions and will not encourage my child to join platforms where they are below the minimum age (under 13 currently for most social media platforms). I will actively monitor my child's out-of-school digital interactions, such as WhatsApp or gaming group chats, to help prevent child-on-child abuse from spilling into school.
- **Privacy & Covert Recording:** Taking secret photos, videos, or recordings of teachers or pupils (including remotely or via wearable technology) is strictly forbidden. Personal recording devices like smart glasses are prohibited without written permission from the DSL. To request a recording, I will speak to the DSL.



- **Visiting School Premises:** I will keep my personal technology in my pocket when visiting the school. I will never share photos or videos of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school will only use my child's image publicly with my explicit consent.

4. ARTIFICIAL INTELLIGENCE & REPORTING

- **Generative AI Risks:** I will talk to my child about the risks of Artificial Intelligence, which is now embedded in many mainstream apps. I will discuss the specific dangers of AI chatbots, image creators, and "nudifying" apps that create inappropriate or illegal content. Advice can be found at parentsafe.lgfl.net.
- **Reporting Without Fear:** I understand that my child may be subject to school sanctions if they break online rules. However, I will reassure my child that they can always tell a trusted adult at home or at school if something goes wrong or upsets them online, without fear of immediate device confiscation or punishment.
- **Further Support:** For comprehensive support on parental controls, safe settings, gaming, apps, and sensitive topics (including cyberbullying, radicalisation, or inappropriate content), please utilise parentsafe.lgfl.net.

PARENT/CARER ACKNOWLEDGEMENT

I/we have read, understood, and agree to support this Acceptable Use Policy.

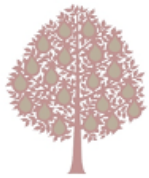
- **Signature(s):** _____
- **Name(s) of Parent / Guardian:** _____
- **Parent / Guardian of (Child's Name):** _____
- **Date:** _____

You can review individual sections of our broader school policy regarding online safety here: https://www.perryfields-jun.essex.sch.uk/page/school-policies/137246.

18. Appendix 3: Acceptable Use Policy for Staff, Governors and Volunteers



Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS



INTRODUCTION & BACKGROUND

We ask everyone involved in the life of Perryfields Junior School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to read, understand, follow, and sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. https://www.perryfields-jun.essex.sch.uk/page/school-policies/137246

If you have any questions about this AUP or our approach to online safety, it is your responsibility to please speak to Samantha Edwards (Headteacher) or Rebecca Kingston (Digital and Online Safety Lead).

By signing this document, I agree to the following:

1. Safeguarding & Reporting

- I have read and will follow the school's Online Safety policy (https://www.perryfields-jun.essex.sch.uk/page/school-policies/137246) and KCSIE Part 1.
- I understand that online safety is a core part of safeguarding. I will report any concerns, inappropriate behaviour, or child-on-child abuse to the Designated Safeguarding Lead (DSL) or Headteacher (in the case of concerns about colleagues) immediately.
- I will use supportive, practical methods to teach online safety and will avoid victim-blaming language.
- I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.

2. Device, System, & Data Security

- I will keep my passwords secret, use Multi-Factor Authentication (MFA) where required, and lock my screen when leaving my device unattended.
- I will check with Samantha Edwards or Rebecca Kingston if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.
- I will report any accidental data leaks or suspected phishing emails to Samantha Edwards or Rebecca Kingston immediately as per the school's Cybersecurity and Data Protection Policies (https://www.perryfields-jun.essex.sch.uk/page/school-policies/137246) without fear of penalty.
- I will not attempt to bypass the school's security, filtering, or monitoring systems.
- I will not use a mobile hotspot to provide internet access to any school device.



- I understand that all my activity on school systems and devices is monitored and can be reviewed by authorised staff.

3. Professional Conduct & Communication

- I will use only official approved platforms for school business and communication. I will not use personal email, WhatsApp, or personal social media for school purposes. WhatsApp groups may be used by staff and governors for appropriate school-related communication, provided that all data protection, confidentiality and safeguarding policies and procedures are followed.
- I will never contact pupils through personal channels and will report any pupils who attempt to do so.
- I will maintain a professional online presence, review my privacy settings, and refrain from posting negative or threatening comments.
- I will disclose any pre-existing personal relationships with pupils or their families to the DSL/Headteacher as soon as possible.

4. Photos, Video, & AI

- I will keep my personal mobile phone turned off and out of sight when in the presence of children.
- I understand it is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device. Other personal recording devices and wearable technology such as smart glasses are not permitted in school without written permission from Samantha Edwards.
- I will only use pre-approved Artificial Intelligence (AI) platforms via my school email account, ensuring my use is ethical, legal, and transparent.
- I will always check the accuracy, quality, and safety of any Gen AI outputs, including from search engine results, before sharing with others, especially children.

5. Supervising Pupils

- I will physically monitor and guide pupils when they are using devices or the internet in the classroom.
- I will prepare and check all online resources and videos for appropriateness (including checking for adverts) before showing them to pupils.
- I will educate pupils about online risks, critical thinking, and the "4 Cs" of online risk: Content, Contact, Conduct, and Commerce.
- I will make the most of teachable moments as they arise in the classroom to promote online safety and digital literacy.

6. Acceptable Use

- I will never use school devices or networks to access illegal, extreme, or inappropriate material.
- I will not support or promote extremist organisations or materials.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Declaration

I have read, understood, and agreed to this policy.

Name: _____

Role: _____

Signature: _____

Date: _____

19. Appendix 4: Acceptable Use Policy for Visitors and Contractors

Acceptable Use Policy (AUP) for VISITORS & CONTRACTORS

INTRODUCTION & BACKGROUND

We ask all children and adults involved in the life of Perryfields Junior School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media.

Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask the Designated Safeguarding Lead (Mrs Edwards)

Further details of our approach to online safety can be found in the overall school Online Safety Policy.

If you have any questions during your visit, you must ask the person accompanying you, Mrs Edwards (DSL) or Miss Kingston (Digital and Online Safety Lead).

If questions arise after your visit, contact Mrs Edwards (DSL) or Miss Kingston (Digital and Online Safety Lead) through the school office.

By signing this document, I agree to the following rules:

1. Interacting with Pupils

- I will not initiate contact, communicate with, or arrange meetings with pupils, face to face or via any technology.
- I will report any safeguarding concerns or inappropriate behaviour immediately to the Headteacher/ Designated Safeguarding Lead (DSL) (Mrs Edwards).

2. Phones, Cameras & Recording

- I will keep my personal mobile phone turned off and, in my pocket, when in the presence of children.
- I will not take photographs, videos, or audio recordings of the school, staff, or pupils without explicit permission from the Headteacher.
- I understand that Smart glasses and all other secret recording devices are strictly forbidden.

3. Using Devices & Networks

- I understand that I can connect personal or work devices only to the designated Guest Wi-Fi. I will not use personal mobile hotspots.
- If provided with school devices or network access, I will use them exclusively for the assigned task. I will not attempt to access pupil or staff data.
- I must lock your device screen when unattended.



- I will not access or view any material that is illegal, extreme, or inappropriate for an educational setting (e.g., adult content). I am aware that all network activity is monitored.

4. Data Privacy & AI

- I will not share my passwords or use another person's login details.
- I will report any accidental data leaks, lost devices, or suspicious emails to the school immediately.
- I will not input any personal or sensitive school data into Generative AI platforms (including AI note-takers).
- All new apps or platforms I use must be approved first by Mrs Edwards or Miss Kingston.
- I will keep all information learned about the school or its community confidential, and will not share or post negative comments about the school on social media.
- I will always check the accuracy, quality and safety of any Gen AI outputs, including from search engine results, before sharing with others, especially children.

Declaration I have read and agree to follow these rules. I understand that failure to do so may result in termination of my contract or visit.

Name: _____

Company/Org: _____

Signature: _____

Date: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name / role / date / time: _____

20. Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**