The Buckinghamshire Primary Pupil Referral Unit

Perseverance Respect Understanding

The Buckinghamshire Primary PRU

E-safety Policy

This policy was agreed by the Management Committee: Autumn 2025

This policy will be reviewed by: Autumn 2026

CONTENTS

1.1 Introduction

At the Buckinghamshire Primary Pupil Referral Unit (PRU) we understand the responsibility to educate our pupils on E-safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

1.11 The PRU will work to educate and empower its staff, parents/carers, pupils and beyond to use the internet as an essential tool for lifelong learning.

1.12 This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2025 and Prevent Duty guidance, in conjunction with the PRU's Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Conduct and Discipline Policy, General Data Protection Regulations Policy, Password Policy and Code of Conduct.

1.13 The purpose of this E-safety Policy is to:

- Safeguard and protect all members of the PRU community online
- Identify approaches to educate and raise awareness of online safety
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns

2.1 Policy Scope

The PRU identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Online safety is an essential part of safeguarding and the PRU acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

2.11 This policy applies to all staff including the management committee, senior leadership team, teachers, support staff, external contractors/visitors and other individuals who work for, or provide services on behalf of the PRU, as well as pupils, parents and carers.

2.12 This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with PRU-issued devices for use off-site, such as work laptops, tablets or mobile phones.

2.13 This policy, supported by the PRU's Code of Conduct and Passwords policies, is to protect the interests and safety of all staff, pupils, parents and carers.

3.1 Roles and Responsibilities

The Headteacher has overall responsibility for safety (including E-safety) within the PRU and reports to the Management Committee. However, the day-to-day management of this will be delegated to the Designated Safeguarding Lead (DSL) who may liaise with other members of staff or other agencies, as appropriate.

Role	Responsibility
Members	• Approval and effectiveness of policy • Member delegated to act as IT/E-safety link • IT/E-safety member updated with any E-safety issues and reports back to management committee
Headteacher and Senior Leadership Team (SLT)	• Ensure that all staff receive suitable CPD to carry out their roles • Ensure there are appropriate and up-to-date policies regarding online safety and that these are implemented ▪ Ensure that the PRU infrastructure/network is as safe and secure as possible ▪ Ensure that online safety is embedded within a progressive curriculum, which enables all pupils to develop an age-

	appropriate understanding of online safety ▪ Support the DSL by ensuring that they have sufficient time and resources to fulfil their online safety responsibilities ▪ Follow the correct procedure in the event of an E-safety concern or incident • Audit and evaluate online safety practice to identify strengths and areas for improvement • Update the IT/E-safety member with any E-safety issues/information
Designated Safeguarding Lead	• Work alongside the ADSLs and IT Manager to ensure online safety is recognised as part of the PRU's safeguarding responsibilities and that a coordinated approach is implemented • Ensure all members of staff receive regular, up-to-date and appropriate online safety training • Access regular and appropriate training to ensure they have up to date knowledge and understand the risks associated with online safety and the additional risks that pupils with SEN and disabilities (SEND) face online • Keep up-to-date with current research, legislation and trends regarding online safety and communicate this, as appropriate • Maintain records of online safety concerns, as well as actions taken, as part of the PRU safeguarding recording • Report online safety concerns, as appropriate, to SLT • Work with SLT, the IT Manager and lead learner for Computing to review and update online safety policies on a regular basis
IT Manager (in conjunction with the current IT provider)	• Provide technical support to the DSL and SLT, especially in the development and implementation of appropriate online safety policies and procedures • Implement appropriate security measures including encryption and safe passwords to ensure that the PRU's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised • Keep up-to-date with current research, legislation and trends regarding online safety, and communicate this as appropriate • Ensure that appropriate filtering is applied and updated through communication with our broadband supplier via Buckinghamshire Council • Report online safety concerns, as appropriate, to SLT • Work with the DSL, SLT and lead learner for Computing to review and update online safety policies on a regular basis
Lead learner for Computing	• Work with the DSL, SLT and IT Manager to review and update online safety policies on a regular basis • Select those parts of the curriculum to deliver in discrete lessons and those that can be covered cross curricular (e.g. within PSHE) • Create exemplar plans for teachers to adapt to their pupils when teaching Computing • Provide support and training for staff so they are confident in delivering Computing lessons

	• Audit resources to ensure they are still fit for purpose and in good working order • Remain up to date with current trends and risk factors in E-safety • Share updates with staff on developments in Computing and E-safety (including dates of Internet Safety for parents' workshops through NSPCC)
Teachers and Support Staff	• Read and adhere to the E-safety Policy and Code of Conduct • Take responsibility for the security of the PRU systems and hardware and the data they use or have access to • Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site • Embed online safety education in curriculum delivery, wherever possible • Have an awareness of a range of online safety issues and how they may be experienced by the children in their care • Identify online safety concerns and take appropriate action by following the PRU safeguarding policies and procedures • Know when and how to escalate online safety issues, including signposting to appropriate support both internally and externally • Take personal responsibility for professional development in this area by participating in appropriate training
Pupils	• Engage in age-appropriate online safety education opportunities • Read and sign the Pupil's Code of Conduct as part of the inreach paperwork • Respect the feelings and rights of others, both on and offline • Take responsibility for keeping themselves and others safe online • If there is a concern online, seek help from a trusted adult and support others that may be experiencing online safety issues • Understand that the E-safety Policy covers actions out of school that are related to the PRU
Parents and Carers	• Role model safe and appropriate use of technology and social media • Read and adhere to the home-school agreement and Code of Conduct • Identify changes in behaviour that could indicate that their child is at risk of harm online • Report any E-safety issues to a member of SLT if they or their child encounter risk or concerns online that relate to the PRU • Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

4.1 E-safety Education

The PRU will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:

4.11 Ensuring education regarding safe and responsible use precedes internet access.

4.12 Including online safety in Personal, Social, Health and Economic (PSHE) lessons, Relationships and Sex Education (RSE) lessons and through computing programmes of study.

4.13 Reinforcing online safety messages whenever technology or the internet is in use and during informal conversations at break and lunch time.
4.14 Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
4.15 Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The PRU will support pupils to read and understand the Code of Conduct by:

4.16 Discussing acceptable use of equipment and the Internet within the first two weeks of placement with a reminder prior to any use of equipment.
4.17 Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
4.18 Rewarding positive use of technology.
4.19 Providing online safety education and training.
4.110 Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Pupils

4.112 The PRU recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an Additional Language (EAL) and children experiencing trauma or loss.
4.113 The PRU will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
4.114 When implementing or reviewing an appropriate online safety policy and curriculum, the PRU will seek input from the SENCo and DSL.

5.1 Staff Training and Engagement

The PRU will**:**

5.11 Provide the E-safety Policy, Password Policy and Code of Conduct to all members of staff as part of induction.
5.12 Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be as part of existing safeguarding training/updates and within separate or specific online safety sessions.
5.13 Make staff aware that our IT systems are monitored; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
5.14 Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
5.15 Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
5.16 Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting staff, pupils, parents and carers.

6.1 Parents/Carers Awareness and Engagement

The PRU recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:
6.11 Providing information and guidance on online safety in a variety of formats.
6.12 Drawing their attention to the E-safety Policy and signing the Code of Conduct provided within our home school agreement.

7.1 Technology

Filtering and Monitoring

7.11 The PRU has appropriate filtering in place which blocks the appropriate categories in line with Keeping Children Safe In Education and the Prevent Duty. The filtering system is updated as new sites become available, blocking a range of unlawful material.
7.12 Visitors read and sign the Visitor Use of the Internet form before being given access to our wireless network.
7.13 All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.
7.14 All pupils will be supervised and adult-directed to online tools.
7.15 The PRU's filtering blocks sites which can be categorised as: pornography, racial hatred, cryptocurrency, extremism, gaming and sites of an illegal nature, in line with Keeping Children Safe In Education and the Prevent Duty.

In the event of a pupil or staff discovering an unsuitable site, they will be required to:

7.16 Turn off monitor/screen and report the concern immediately to a member of staff.
7.17 The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or IT Manager.
7.18 The breach will be recorded and escalated as appropriate.
7.19 Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Police or CEOP.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems. This includes:

7.110 Virus protection installed on all PRU devices and being updated regularly.
7.111 Encryption when accessing PRU hardware and for sending personal data sent over the internet.
7.112 Not attempt to bypass or alter any security settings on devices.
7.113 Not using USBs or portable media without specific permission.
7.114 Not install or download unapproved software to work devices or opening unfamiliar email attachments.
7.115 Regularly checking files held on our network.
7.116 All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private and updated regularly.
7.117 Users have clearly-defined access rights to parts of the PRU network.

Managing Personal Data Online

7.118 Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our General Data Protection Regulations Policy.

Use of digital and video images

7.120 We allow staff to take images to support educational aims, but follow guidance in the home/school agreement concerning distribution and publication of those images.
7.121 Written permission is sought from parents/carers before images or videos of pupils are displayed or published.

Managing Email

7.122 Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
7.123 PRU email addresses and other official contact details will not be used for personal use or for setting up personal social media accounts.
7.124 Staff will immediately inform the DSL or IT Manager if they receive offensive communication, and this will be recorded in our safeguarding records.

Staff email

7.125 The use of personal email addresses by staff for any official PRU business is not permitted.
7.126 All members of staff are provided with an email address to use for all official communication.
7.127 Staff email addresses are used solely for PRU business and not for personal use.
7.128 Digital communication between staff and other professionals and parents/carers is professional in tone and content.
7.129 Members of staff are encouraged to have an appropriate work/life balance when responding to email.

Educational use of Videoconferencing

The PRU recognises that videoconferencing can be a challenging activity but brings a wide range of learning benefits and allows access to learning between PRU sites.

7.130 All videoconferencing equipment will be switched off when not in use.
7.131 Videoconferencing contact details will not be posted publicly.
7.132 Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
7.133 Parents/carers consent is obtained in the Inreach Agreement Consent Form.
7.134 Video conferencing will take place via official and approved communication channels.
7.135 The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely to prevent unauthorised access.

Management of software used to record children's progress

7.136 The PRU uses a number of online software packages to support and record pupil progress. These packages are used in accordance with the General Data Protection Regulations (GDPR) and Data Protection legislation.

8.1 Reducing Risks

The PRU recognises that the internet is a constantly-changing environment with new apps, devices, websites and material emerging at a rapid pace. As a result, we will ensure that we carry out the following:

8.11 Regularly review the methods used to identify, assess and minimise online risks.
8.12 Review emerging technologies for educational benefit and undertake appropriate risk assessments before use in the PRU is permitted.
8.13 Ensure that there is appropriate filtering and take all reasonable precautions to ensure that users can only access appropriate material.
8.14 Ensure that appropriate security measures are in place to protect servers, firewalls, wireless systems and hardware from accidental or malicious attempts which might threaten the security of the PRU systems.

However, due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

8.15 All staff and pupils are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the PRU.

8.16 All staff must respect the work and ownership rights of people outside of the PRU and abide by copyright laws.

9.1 Social Media

Social Media Expectations

The expectations regarding safe and responsible use of social media applies to all members of the PRU.

9.11 The term 'social media' may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming, including the use of messaging and within-game chat functions; apps; video/photo sharing sites; chatrooms and instant messengers.

9.12 Concerns regarding the online conduct of any member of the PRU on social media, should be reported to the DSL and will be managed in accordance with our Anti-bullying, Allegations Against Staff, Behaviour and Safeguarding Policies.

Staff Personal Use of Social Media

9.13 The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff via regular staff training opportunities.

9.14 All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.

9.15 Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

9.16 All members of staff are advised to safeguard themselves and their privacy when using social media sites.

9.17 Members of staff are encouraged not to identify themselves as employees of the PRU on their personal social networking accounts; this is to prevent information on these sites from being linked with the PRU and to safeguard the privacy of staff members.

9.18 All members of staff are encouraged to carefully consider the information, including text and images that they share and post online and to ensure that their social media use is compatible with their professional role. It must also be in accordance with our policies and the wider professional and legal framework.

9.19 Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.

9.110 Members of staff will notify the senior leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

9.111 All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.

9.112 Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted. Any communication from pupils and parents received on personal social media accounts will be reported to the Headteacher or DSL.

Pupils Personal Use of Social Media

9.113 Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach.

9.114 Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

9.115 Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:

9.116 To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

9.117 To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

9.118 Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

9.119 To use safe passwords and not to share them or leave details where others may see them.

9.120 To use social media sites which are appropriate for their age and abilities.

9.121 How to block and report unwanted communications.

9.122 How to report concerns both within the setting and externally.

10.1 Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures such as: Safeguarding, General Data Protection Regulations and Code of Conduct.

Staff will be advised to:

10.11 Keep mobile phones in a safe and secure place outside of the classroom.

10.12 Not use personal devices during teaching periods, unless permission has been given by the Headteacher as in emergency circumstances.

10.13 Not use their own personal phones or devices for contacting pupils or parent/ carers. Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher or DSL.

Staff will not use personal devices:

10.14 To take photos or videos of pupils and will only use work-provided equipment for this purpose.

10.15 Directly with pupils and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our Code of Conduct and Conduct and Discipline Policy. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the Police will be contacted.

Pupils Use of Personal Devices and Mobile Phones

10.16 The PRU expects pupils' personal devices and mobile phones to be switched off and handed to the main office upon arrival. The devices are not to be switched on again until they have left the PRU site.

10.17 Any misuse of personal devices and mobile phones will be dealt with in accordance with our Safeguarding, Behaviour or Anti-bullying Policies.

10.18 Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.

10.19 If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the Police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

10.110 Parents/carers and visitors (including other professional agencies) must use their mobile phones and personal devices in accordance with our Code of Conduct and other associated policies, such as: Anti-bullying, Behaviour, Safeguarding and General Data Protection Regulations.

10.111 Parents/carers and visitors must not use their personal devices or mobile phones around pupils or within class.

10.112 We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

10.113 Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL or site lead of any breaches of our policy.

11.1 Reporting Online Safety Incidents and Concerns

11.11 All members of the PRU will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

11.12 All breaches of personal data must be reported to the Data Protection Lead who will report these to the Data Protection Officer and record on the Data Breach record.

11.13 All members of the PRU must respect confidentiality and the need to follow the official procedures for reporting concerns.

11.14 Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

11.15 We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.

11.16 After any investigations are completed, staff will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

11.17 The PRU will follow the NSPCC guidance on when to contact the Police.

Concerns About Pupils' Welfare

11.18 The DSL will be informed of any online safety incidents involving safeguarding or safeguarding concerns.

11.19 The DSL will record these issues in line with our Safeguarding Policy.

11.110 The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the DSCP thresholds and procedures.

11.111 We will inform parents and carers of online safety incidents or concerns involving their child as and when required.

Staff Misuse

11.112 Any complaint about staff misuse will be referred to the Headteacher, in accordance with the Safeguarding Policy.

11.113 Issues which do not meet the threshold requiring reporting to the LADO (Local Authority Designated Officer) will be recorded in the PRU's record of low-level concerns.

11.114 Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer).

11.115 Appropriate action will be taken in accordance with our Code of Conduct and Conduct and Discipline Policy.

12 Useful Links

CEOP Education from the National Crime Agency https://www.thinkuknow.co.uk/
Childnet: https://www.childnet.com/
National Online Safety: https://nationalonlinesafety.com/
Internet Matters: https://www.internetmatters.org/
Better Internet for Kids: https://www.betterinternetforkids.eu/en-GB/
Internet Watch Foundation (IWF): https://www.iwf.org.uk/
NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
UK Safer Internet Centre: https://saferinternet.org.uk/
Parent Zone: https://parentzone.org.uk/library
UK Government: https://www.gov.uk/society-and-culture/online-safety

Signature:
Chair of Management Committee Date:

Headteacher

Signature: Date: