Castle Phoenix Trust

Online Safety & Cyber Security Policy

Trust Level Policy

Date effective	September 2025
Review Cycle	Annually
Review Date	September 2026
Date of Approval by Trustees	12 November 2025
Committee approved by	Trust Board
Author	Alex Handy

Date	Notes

This Trust policy applies to all our schools

1. Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. In order to ensure that the school provides a safe environment for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding and our schools have a duty to ensure that all pupils and staff are protected from potential harm online
- Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online

The purpose of the online safety policy is to:

- Safeguard and protect all members of our schools' community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to 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.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material; for example, pornography, racist or radical and extremist views, and in some respects fake news
- Contact: being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them
- Commercial exploitation: for example, young people can be unaware of hidden costs and advertising in apps, games and website
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying

2. Policy Scope

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

It applies to all schools *within the Castle Phoenix Trust (CPT)* including the Early Years Foundation Stage *(EYFS).*

It applies to access to school systems, the internet and the use of technology, using devices provided by the school or personal devices at all times whilst engaged on school business or activity or whilst on school premises.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2.1 Links with other policies and practices

This policy links with a number of other policies, including:

- The Data Protection Policy
- The school's Safeguarding and Child Protection Policy
- Safeguarding Procedures (which incorporates the staff Code of Conduct)
- Acceptable Use Processes
- The school's Behaviour policy
- Anti -bullying policies in schools

3 Roles and Responsibilities

- **Alex Handy** is the Trust Online Safety Lead (CPT OSL) responsible for online safety and cyber security oversight across our schools.
- **School based** Designated Safeguarding Leads (DSLs)_ have responsibility for online safety unless a deputy has been designated for this specific role
- All members of the community have important roles and responsibilities to play with regard to online safety:
- Online- safety forms part of the responsibility of the local governor link for safeguarding
- The Trustee link for Safeguarding, Mick Michael, on behalf of the Trust Board has responsibility for monitoring this policy and should be alerted to any aspect of concern through liaison with Alex Handy

3.1 The Headteacher:

- Has overall accountability for online safety provision
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with CPT and national recommendations and requirements
- Ensures the school follows CPT policies and practices regarding online safety and cyber security (including the Acceptable Use Processes), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, CPT and national support
- Receives regular reports from the DSL on online safety
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

The DSL/On line Safety Lead in schools:

- Takes lead responsibility for online safety (including understanding and filtering and monitoring processes and systems in place)
- Promotes an awareness of and commitment to online safety throughout the school community
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Monitors pupil internet usage, taking action where required
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends using the CPOMs system
- Reports regularly to the Headteacher and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.

3.3 Staff managing the technical environment:

- Apply appropriate technical and procedural controls to ensure that the school'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 the Trust's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures
- Ensure that the school's filtering policy is applied and updated on a regular basis, and oversees the school's monitoring system
- Report any filtering breaches or other online safety issues to the CEO, Headteacher, CPT OSL and other bodies, as appropriate
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.
- Adheres to the main components of Cyber Essentials

3.4 All school staff:

- Read, adhere to and help promote the online safety policy, Acceptable Use Processes and other relevant school policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Model safe, responsible and professional behaviours in their own use of technology
- Embed online safety in their teaching and other school activities
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant)
- Have an up-to-date 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 reporting to the DSL
- Know when and how to escalate online safety issues
- Take personal responsibility for professional development in this area.

3.5 Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age-appropriate online safety education opportunities
- Read and adhere to the school Acceptable Use Processes
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online

3.6 Parents and carers:

- Read the school Acceptable Use Processes on the school website and encourage their children to adhere to them
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home

- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Use school systems, such as learning platforms, and other network resources, safely and in accordance with this on line safety policy
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

3.7 External groups:

- Any external individual/organisation must sign an Acceptable Use Agreement *(AUA)* prior to being given individual access to the school network

4.1 Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of what they see online and shown how to validate information before accepting its accuracy
- Teaching pupils to respect and adhere to principles of academic integrity. This will include understanding the importance of producing their own independent work, being transparent and honest about any use of source material or generative applications, respecting copyright and using appropriate referencing conventions
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:

- Discussing the Acceptable Use Agreement, the BYOD Code of Conduct (where appropriate) and their implications, and reinforcing the principles via display, classroom discussion etc.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Recognising positive use of technology by pupils.

4.2 Training and engagement with staff employed by school and our Trust

- All new staff members will receive training, as part of their induction, on cyber security, safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive online safety refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through the National Online Safety portal, emails, e-bulletins and staff meetings).
- 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.
- Trustees will receive cyber security training yearly.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.
- Make staff aware that school systems are monitored and activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

4.3 Awareness and engagement with parents and carers

Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings
- Informing parents about what the school asks pupils to do online, and who they will be interacting with
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website
- Requiring parents to read the pupil Acceptable Use Agreement and discuss its implications with their children.

5. Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The Trust and school will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

- Ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not

6. Safer Use of Technology

6.1 Classroom Use

- The school uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platforms
    - Cloud services and storage
    - Email and messaging
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
    - Virtual reality headsets
    - Generative artificial intelligence
    - Supervision of pupils will be appropriate to their age and ability
    -
- All devices should be used in accordance with the online Safety Policy, the school's AUAs and with appropriate safety and security measures in place.
- Members of staff should always thoroughly check websites, tools and apps for suitability before use in the classroom or recommending for use at home
- Staff and pupils should consider copyright law and principles of academic integrity before using internet-derived materials (and where appropriate comply with licence terms and/or acknowledge the source of information).

6.2 Filtering and Monitoring

- Schools operates on a single network, with a connection to the internet that is managed by a firewall. This firewall inspects internet traffic to block malware and many other threats. The firewall also blocks access to and from a number of harmful and malicious websites. The firewall access rules are managed centrally by the IT team at Caludon
- In addition to the firewall, CPT uses an internet filtering solution that provides the ability to filter or block websites visited by users on any CPT managed device, whether on or off the CPT IT network. The system also provides in depth monitoring, analysis and reporting on activity by users on all CPT managed devices.
- For the vast majority of CPT devices the system generates flags when defined keywords are used or generates alerts when the system identifies patterns of behaviour that warrant further action. For all IT CPT uses *a* fully managed system to monitor staff and student activity.
- CPT also uses an email gateway that manages and filters all inbound and outbound email traffic to protect users from malicious email threats. All members of staff are however 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
- All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

6.3 Dealing with Filtering breaches

The schools have a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to alert a member of staff immediately

- The member of staff will report the concern (including the URL of the site if possible) to the DSL
- The breach will be recorded and escalated as appropriate
- Any material that the Trust/School believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

6.4 Managing Personal Data Online

Personal data will be collected, processed, stored and transferred in accordance with the General Data Protection Regulations and the CPTs Privacy Notices. Full information can be found in the school's Data Protection Policy.

Social Media

7.1 Expectations

- The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times

7.2 School and Trust Staff Use of social media

The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities

- Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct, staff Acceptable Use Agreement and Social Media Policy

7.3 Pupils' Personal Use of social media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age
- The school will control pupil access to social media whilst using school-provided devices and systems on site
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

8. Use of Personal Devices and Mobile Phones

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

8.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-Bullying, Behaviour and Discipline, and Safeguarding and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage or breach of security of such items on school premises
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms, toilets and swimming pools. Bring Your Own Device (BYOD) laptops may be used according to the BYOD Code of Conduct. Mobile phones may only be used during the school day by Sixth Form students in accordance with the Mobile Phone Policy.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the school community; any breaches will be dealt according to the behaviour policy
- All members of the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Safeguarding and Child Protection policies.

8.2 School and School Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child Protection, Data Security and Acceptable Use Processes.
- Personal digital recording devices ***must*** not be used for taking, editing or transferring images or videos of pupils. This restriction also applies in our EYFS settings.

8.3 School and Trust Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. Multi Factor Authentication (MFA) must be enabled on all accounts when being used outside of the school's network
- If staff have any concerns over the security of their device, they must seek advice from the Network manager

8.4 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences
- Pupils' personal devices and mobile phones are to be used in line with individual school's Mobile Phone Policy and BYOD Code of Conduct.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place
- Searches for and of mobile phone or personal devices will only be carried out in accordance with the relevant government guidance
- Schools are not required to inform parents before a search takes place or to gain consent for a search for a prohibited item, or item which a member of staff reasonably suspects has been or is likely to be used to commit an offence or to cause personal injury or damage to the property of any person

8.5 Visitors' Use of Personal Devices and *Mobile Phones*

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Agreement and other associated policies, such as online safety, Anti-Bullying and Safeguarding and Child Protection policies whilst on school premises, engaged on school business or connected to the school network
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

9. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), self-generated images of sexual abuse as a result of online grooming, cyberbullying and illegal content
- All members of the school community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the CPT OSL.
- Where there is suspicion, that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised

9.1 Concerns about Pupils' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

9.2 Misuse

- Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint
- Any complaint about staff misuse will be referred to the Headteacher or in the case of the Head to the Chair of Governors
- Pupils and parents are informed of the school's complaints procedure.

9.3 Examining electronic devices

Schools have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

10. Monitoring and Review

- Schools will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice
- The policy framework will be reviewed by CPT at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place

11 Security

Password Security

Staff members must adhere to the CPT password policy all online services which uses their staff credentials. The policy is:

1. 8 characters
2. One number
3. One special character
4. One capital

11.1 External USB storage devices

Staff members should not use USB storage devices either in the form of "memory sticks" or "external hard drives". Where there is no alternative e.g., exams officers a social access request will need to be put in with the Headteacher or designated DCL

11. Useful links and sources of advice

11.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: understand, prevent and respond (Child net)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Self-generated child sexual abuse (IWF)
- Meeting digital and technology standards in schools and colleges March 2022 (DfE)
- Generative artificial intelligence in education (DfE)

11.2 National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk

- Child net: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Telephone helpline: 0844 381 4772

11.3 Parents Guidance

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

- What are the issues? - https://nationalonlinesafety.com
- Hot topics - Child net International
- Parent factsheet - Child net International

Educating parents about online safety and cyber security

The school will raise parents' awareness of internet safety and cyber security through the National Online Safety portal. This policy will also be made available for parents.

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

11.4 Legislation and guidance

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

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education –
- Searching, screening and confiscation

It also refers to the Department'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 considers the National Curriculum computing programmes of study.

Cyber Security

DFE-Cyber Security standards for schools and colleges

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

National Cyber Security Centre

https://www.ncsc.gov.uk/section/education-skills/schools

National Online Safety

https://nationalonlinesafety.com