Castle Phoenix Trust

Online Safety, Acceptable use, and Cyber Security Policy

Trust Level Policy

Date effective	August 2023
Review Cycle	One Year
Review Date	June 2024
Date of Approval by Governors	To be Ratified
Committee approved by	HRG/Board of Trustees
Author	Alex Handy

Date	Notes

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) effective 25 May 2018

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors and that the cyber security of the Trust is maintained.
- Deliver an effective approach to online safety and cyber security, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an online safety and cyber security incident, where appropriate

2. Legislation and guidance

Online Safety

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 takes into account 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

3 Roles and responsibilities

3.1 The governing board

The trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governor who oversees online safety is Brian Sedgebear.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher and SLT

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

The headteacher and SLT (Designated Cyber Lead, DCL) are responsible for ensuring that their network leads are following due diligence regarding cyber security within Trust procedures and that their staff understand this policy and are trained yearly in cyber security.

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, SLT, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network manager

Online Safety

The Network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Cyber Security

- Ensuring that the school complies with the technical components of Cyber Essentials which includes the following elements:

Process, Understanding Hardware, Understanding The Environment, Boundary Protection, Secure Configuration, User Access Control, Administration Access Control, Password Based Authentication, Patch Management, Data Protection, Remote Access.

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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL and DCL to ensure that any online safety and cyber security incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure 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 can seek further guidance on keeping children safe online from the following organisations and websites:

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

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

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

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

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

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. 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/ DCL.

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 one 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 are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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/ ACHIEVE programme) 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 §so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff 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.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices). 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.

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons (unless specifically asked by the teacher to do so)
- Tutor group time

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

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

Students who have signed up the 1:1 iPad scheme can user their devices in lesson, under instruction from their classroom teacher. These devices are centrally managed by our MDM solution.

Staff

9. Personal Use

The main purpose for the provision of ICT facilities by the school is for use in connection with the approved business activities of the school. The school permits the use of its ICT facilities by employees and other authorised users subject to the following limitations:

The level of usage will not be detrimental to the main purpose for which it is provided, i.e. School business, and priority will be given to the use of resources for this main purpose.

Personal use must not be of a commercial or profit-making nature or for any other form of personal financial gain and must not be of a nature that competes with the school's business or results in unauthorised expenditure to the school, eg excessive printing.

Personal use must not be connected with any use or application that conflicts with an employee's or user's obligations to the school, or with any of the Trust's policies or procedures and must comply with all such policies and procedures.

The school recognises that employees occasionally need to deal with domestic and family needs during working hours. Employees may use office telephones, business mobiles (and similar devices) or email for such purposes providing the level of usage does not affect their level of performance or conflict with school business.

The policy is to enable employees to manage essential family and domestic issues and is not to enable employees to maintain social contacts during working hours e.g. on-line social chatting. The private use of school facilities should be kept to a minimum. This also applies to incoming calls.

Personal calls to premium rate lines are unacceptable.

Personal international calls should only be made if the employee is travelling abroad for work commitments and any such calls should be kept to a minimum.

Extended personal conversations via telephone or email, use of chat rooms and non-work related Internet browsing will not be permitted within working hours.

Where an employee's level of performance is affected by unreasonable personal use of the school's ICT facilities or where abuse of the school's facilities is identified, disciplinary action may be taken and repayment of call costs may be required. Line managers are responsible for promoting good practice and ensuring that employees are aware of this policy.

10. Installation of Software

For the protection of employees and users, the Trust prohibits employees and users from installing software onto their PCs. This includes software that could be downloaded, installed or run from the Internet, for example files that have a name ending in .exe or .com, as these may introduce viruses or code to the system. Where software is required for school business prior authorisation must be sought from your line manager.

11. Password Security

Staff members must adhere to the Trust's 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 letter

10. 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. Use of Telephones

Employees and users have a responsibility to ensure that telephone access, provided to them to enable them to carry out their duties, is not abused. The Trust will undertake periodic monitoring of the use of telephone facilities.

Employees who are required to use a mobile, or similar devices (e.g. Blackberry) for business purposes will be required to declare all private calls and make payment for them. This will include the VAT elements of the call.

The school recognises that from time-to-time employees make business telephone calls on their personal mobile phones. The use of an employee's personal mobile phone should be kept to a minimum and where at all possible landlines used. The school will expect to reimburse the employee for any business calls made on personal mobile telephones. The reimbursement will be the call charge plus VAT. (Where free minutes are used the amount reimbursed will be equivalent to that had there been a charge attached to the call). Employees should keep a record of any business calls and the reason for the call if they wish to be reimbursed.

Managers should not expect employees to utilise their personal phones on a regular basis. Should the need for a mobile phone for business use be identified then appropriate arrangements should be made through the business manager or HR Team. Particular attention should be made to the need for risk assessment where the need for a mobile phone is identified for reasons of safety.

Where use of home telephones and mobile telephones are part of an employee's job, their use and any payments relating to them will be specified as part of the contract.

School telecommunications equipment may be used for essential family and domestic issues providing such use is not excessive and does not conflict with school business or policy.

Such equipment should not be used for maintaining social contact during working hours.

Line Managers have a responsibility to monitor usage and to promote best practice

12. Training

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 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. Governors will also 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.

13. 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, as set out in the appendices.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. 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.

14. 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 ICT and internet acceptable use]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

15. Monitoring arrangements

The DSL/ DCL logs behaviour and safeguarding issues related to online safety on CPOMS or the schools equivalent central record. This record should be accessible to the Trust lead on digital technologies if required.

This policy will be reviewed every year by the trust lead for digital technologies. At every review, the policy will be shared with the governing board.

16. Links with other policies

This online safety/ cyber security policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Acceptable Use Policies (AUP)

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Because of the age groups involved the Trust will use an AUP video for EYFS and KS1 pupils. The AUP below will be signed when the video has been watched.

Appendix 2: KS2, KS3 and KS4/ 5 acceptable use agreement (pupils and parents/carers)

https://forms.office.com/e/hr5qTr3i1J

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

https://forms.office.com/e/3gCc3FGN0G

Appendix 4: online safety incident report logs

All Online Safety and Cyber Security concerns should be logged on the schools' helpdesk system and CPOMS so it can be collated centrally.