Online Safety Policy

Created in: November 2023
Review date: November 2024
Approved by CEO – November 2023

Contents

Rationale

This policy applies to all members of the Trust community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of Trust ICT systems, both in and out of the schools. It also applies to the use of personal digital technology on a school site (where allowed).

Aims

Prince Albert Community Trust (PACT) and its schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, 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 them 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.

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 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 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.

Roles and Responsibilities

Trust Board, CEO and Director of Welfare

The Trust board and CEO has overall responsibility for monitoring this policy and holding Heads to account for its implementation at PACT schools.

The 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 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 board will, through regular meetings with and reporting from the Director of Welfare, discuss online safety, requirements for training, and monitor online safety logs as provided by the Director of Welfare and designated safeguarding leads (DSLs).

The board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The Director of Welfare, working alongside the board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They will review the DfE filtering and monitoring standards, and discuss with ICT staff and service providers what needs to be done to support schools in meeting those 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 their safeguarding needs.

All Trustees, Local Academy Committee (LAC) Representatives and the Director of Welfare will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of PACT ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure 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.

Executive Headteachers, Headteachers and Heads of School
Heads are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout their respective schools.

Designated Safeguarding Leads (DSLs)
Details of each PACT school's designated safeguarding leads (DSLs) are set out in the respective school's Child Protection and Safeguarding policy.

DSLs take lead responsibility for online safety in school, in particular:

- Supporting the head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the Trust ICT Operations Lead to make sure the appropriate systems and processes are in place.
- Working with the head, Trust ICT Operations Lead, Senior ICT Technicians, 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.
- Ensuring that any online safety incidents are logged 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.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the head, LAC and/or the Director of Welfare.
- Undertaking annual risk assessments that consider and reflect the risks children 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.

ICT Support team
The Trust ICT Operations Lead and Trust Cyber Security Lead, supported by the Senior ICT Technicians are 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 ensure pupils are kept 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

All staff (including agency staff and contractors, and volunteers)
All staff, including agency staff and contractors, 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 PACT ICT systems and the internet, and ensuring that pupils/students follow the terms on acceptable use.
- Knowing that the DSLs are responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting both the DSL and ICT Service Desk.
- Following the correct procedures by contacting the ICT Service Desk if they need to bypass the filtering and monitoring systems for educational purposes – this is a request for change.
- Working with the DSL to ensure that any online safety incidents are logged 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents/carers
Parents/carers are expected to:
- Notify a member of staff or the head 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.

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
- Hot topics - Childnet International
- Parent resource sheet - Childnet International

Visitors and members of the community
Community users who access school systems, websites and so on as part of the wider Trust provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Visitors and members of the community who use the PACT 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 (see Community User Acceptable Use Policy) before being provided with access to school systems.

Educating pupils/students about online safety

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.

In Key Stage 1 (KS1), 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 (KS2) 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.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In KS3, students 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.

Students in KS4 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, students 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 partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that 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.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including 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/students with SEND.

Educating parents/carers about online safety

PACT schools will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via the school website. This policy will also be shared with parents/carers. Online safety will also be covered during parents' evenings or events such as parent/carer workshops.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the head.

Cyber-bullying

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.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils/students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils/students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

PACT schools will actively discuss cyber-bullying with pupils/students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups.

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/students, as part of safeguarding training.

Schools also send 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.

Examining electronic devices
The head, and any member of staff authorised to do so by the head, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils/students, 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/students and staff. If the search is not urgent, they will seek advice from the head/DSL.
- Explain to the pupil/student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's/student'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 DSL/head to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if 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/students 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 policy and Search, Confiscation and Screening policy.

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

Artificial Intelligence (AI)
Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils/students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

PACT recognises that AI has many uses to help pupils/students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

PACT will treat any use of AI to bully pupils/students in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust. Unless a full Data Protection Impact Assessment (DPIA) has been carried out for the system in question, personal data must not be entered into an AI tool such as ChatGPT for processing.

Acceptable use of the internet in school

All pupils/students, parents/carers, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the PACT/school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils/students, 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 Appendix A.

Pupils using mobile devices in school

At PACT Primary Schools, pupils are not allowed to bring mobile phones into school.

Students at PA High may bring mobile phones to school; however, they must be switched off before starting school and not switched on again until leaving school. Student mobile phones must not be used during the school day and the school accepts no liability for any loss/damage relating to students' personal mobile phones.

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 are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol).
- 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.
- Not tampering with the pre-installed anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the PACT terms of acceptable use, as set out in appendix A and any equipment loan agreements.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice by contacting the ICT Service Desk.

How we will respond to issues of misuse

Where a pupil/student 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.

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

Training

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, 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 DSLs 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 about online safety at regular intervals, and at least annually.

Trustees and Local Academy Committee Representatives 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 school Child Protection and Safeguarding policies.

Review

This policy will be reviewed annually.

Each academic year, PACT schools will each carry out an annual risk assessment that considers and reflects the risks pupils/students face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly. Heads are responsible for ensuring that these annual risk assessments are completed.