PDET

Online Safety Policy

Date	Revision & Amendment Details	By Whom
January 2026	First draft	Central Team

CONTENTS

This is a Peterborough Diocese Education Trust (PDET / the Trust) Policy and applies to all schools within the Trust.

1. Aims

The Trust aims to:

- Have robust processes in place to ensure the online safety of children, staff and volunteers (including directors and school forum members)
- Identify and support groups of children that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers the Trust to protect and educate the whole Trust community in its use of technology, including mobile and smart technology (which is referred to in this policy 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, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact**: being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and / or financial scams.

2. Legislation and Guidance

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

- *Teaching online safety*
- *Meeting digital and technology standards*
- *Preventing and tackling bullying* and *cyber-bullying: advice for headteachers and school staff*
- *Relationships and sex education (RSE) and health education*
- *Searching, screening and confiscation*

It also refers to the DfE's guidance on *protecting children from radicalisation*.

It reflects existing legislation, including but not limited to the *Education Act 1996* (as amended), the *Education and Inspections Act 2006* and the *Equality Act 2010*. In addition, it reflects the *Education Act 2011*, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on children's 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.

This policy complies with the Trust's funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Trust Board of Directors (Board)

The Board has overall responsibility for monitoring this policy and holding the Trust's Executive (Executive), who in turn hold Headteachers / Principals / Heads of School (headteachers), to account for its implementation.

The Board, acting through the Executive and headteachers, 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
- 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
- Co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding leads (DSLs)
- Make sure that schools teach children how to keep themselves and others safe, including online
- Make sure that schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They will review the *DfE's filtering and monitoring standards*, and discuss with IT service providers what needs to be done to support the schools in meeting the standards, which include:
    - identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - reviewing filtering and monitoring provisions at least annually
    - blocking harmful and inappropriate content without unreasonably impacting teaching and learning
    - having effective monitoring strategies in place that meet the schools' safeguarding needs
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some children 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
- Make sure that online safety is a running and interrelated theme when devising and implementing the Trust's approach to safeguarding and related policies and / or procedures.

All Directors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Trust's ICT systems and the internet as set out in the *Trust's Acceptable Use Policy (AUP)*

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy / deputies (DDSL(s)) are set out in the school's Safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher to make sure the procedures and implementation of this policy are updated and reviewed regularly, in particular following the annual review of this policy
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the headteacher, Trust Central Team 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 *Safeguarding Policy*
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged on MyConcern and dealt with appropriately in line with the *Trust behaviour policy*
- Updating and delivering staff training on online safety (*appendix 2* 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 the Executive
- 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.

3.4 The IT Service Provider (ICT manager)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure children are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the schools' IT 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 schools' IT 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.

3.5 All staff (including Contractors and Agency Staff) and Volunteers (including Directors and School Forum Members)

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 Trust's ICT systems and the internet as set out in the *Trust's AUP*, and making sure that children follow the Trust's and school's terms on acceptable use as set out in the AUP

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing as set out in *appendix 1 - school specific details*
- Following the correct procedures as set out in *appendix 1 – school specific details* if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the *Trust 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.

3.6 Parents / Carers

Parents / Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet as set out in the AUP .

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

- What are the issues? – *UK Safer Internet Centre*
- Help and advice for parents / carers – *Childnet*
- Parents and carers resource sheet – *Childnet*

3.7 Visitors and Members of the Community

Visitors and members of the community who use the Trust's IT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use as set out in the AUP.

4. Educating Children about Online Safety

4.1 Children will be Taught about Online Safety as Part of the Curriculum

In **Key Stage (KS) 1**, children 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.

Children in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content.

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

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues 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 children with SEND.

4.2 Children will be Taught Practical Cyber Security Skills

All children will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach.

Children will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating Parents / Carers About Online Safety

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

Online safety will also be covered during parents' evenings.

The school will let parents / carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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

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

6. Cyber-Bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Trust *behaviour policy*.)

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

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 and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training (see *section 11* for more detail).

The school also sends out information 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 Trust behaviour policy. Where illegal, inappropriate or harmful material has been spread amongst children, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

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

- Poses a risk to staff or children, 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 children and staff.
- Explain to the child why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the children'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 Headteacher in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and / or
- The child 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 children 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*.

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, children and parents / carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Trust recognises that AI has many uses to help children 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Schools will treat any use of AI to bully children very seriously, in line with the school's approach to bullying outlined in the Trust *behaviour policy.*

Staff should be aware of the risks of using AI tools while they are still being developed and should only use those agreed by the Chief Operating Officer.

Any use of artificial intelligence should be carried out in accordance with the Trust's AI policy.

7. Acceptable Use of the Internet in School

All children, parents / carers, staff and volunteers are expected to sign an agreement regarding the acceptable use of the Trust's / school's ICT systems and the internet (see the AUP). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

More information is set out in the AUP.

8. Children Using Mobile Devices in School

Some schools do not permit children to bring mobile devices into school, whilst others permit it on the basis that they are handed into the school office – see *appendix 1 for school specific details.*

9. Staff Using Work Devices Outside School

Use of work devices outside of school is covered in the AUP.

10. How the School will Respond to Issues of Misuse

Where a child misuses the school's ICT systems or internet, the procedures set out in the *Trust policies on behaviour and the AUP* will be followed. 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 *Trust's staff disciplinary procedures / adult code of conduct*. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training for Staff and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and / or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation / hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSL/s 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.

Directors 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 the *Trust's safeguarding policy.*

12. Monitoring arrangements

The DSL and staff log behaviour and safeguarding issues related to online safety on MyConcern.

This policy will be reviewed every year by the Board to consider and reflect the risks children face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to the Trust's:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy
- IT controls policy

Appendix 1 - School Specific Details

Reporting of Any Incidents of Filtering and Monitoring Systems or Processes Failing

Any concerns regarding the failure, suspected failure, or inappropriate functioning of the school's filtering and monitoring systems must be reported immediately.

- Staff should report issues to the **Designated Safeguarding Lead (DSL)** or **IT Support Provider** as soon as they are identified.
- Pupils are encouraged to report any concerns to a trusted adult, class teacher, or a member of the safeguarding team.
- All incidents will be logged, investigated promptly, and appropriate action will be taken to resolve the issue.
- Where required, incidents will be escalated to senior leadership and external providers to ensure compliance with statutory safeguarding duties.
- Any safeguarding concerns arising from system failures will be managed in line with the school's **Safeguarding and Child Protection Policy**.

Procedures for Bypassing Filtering and Monitoring Systems for Educational Purposes

The school recognises that, in limited circumstances, it may be necessary to access content that is normally filtered for legitimate educational purposes.

- Requests to bypass filtering systems must be made in advance by a member of staff to the **Headteacher**, **DSL**, or **IT Lead**.
- Access will only be granted where there is a clear educational rationale and appropriate supervision is in place.
- Temporary access will be time-limited and monitored.
- Pupils will not be permitted to bypass filtering or monitoring systems under any circumstances.
- All such access will be logged and reviewed to ensure continued compliance with online safety requirements.

Mobile Phones

The school recognises both the benefits and risks associated with mobile phone use.

- Pupils are not permitted to use mobile phones during the school day.
- Mobile phones brought into school must be switched off and stored safely as directed by staff.
- The school accepts no responsibility for loss or damage to personal devices.
- Staff mobile phone use is restricted to non-contact time and must not interfere with professional responsibilities or safeguarding duties.
- The use of mobile phones to take photographs, videos, or audio recordings is strictly prohibited unless authorised for educational purposes.
- Any misuse of mobile phones will be managed in line with the school's **Behaviour Policy** and **Acceptable Use Policy**.

Other School-Specific Online Safety Details

- All users of the school's network must comply with the **Acceptable Use Policy**.
- Online safety is embedded within the curriculum and reinforced through assemblies and staff training.
- The school regularly reviews filtering and monitoring arrangements to ensure they remain effective and compliant with statutory guidance.
- Parents and carers are provided with guidance to support safe online behaviour at home.