Policy & Procedure

Newcroft Primary Academy

Aspiring for Excellence

Online Safety Policy 2025v1

This policy was agreed by the governing body on 6th October 2025 and will be reviewed as required.	
Signed:	Chair of Governors
Date: 7th October 2025	

Statutory Policy

1. The aims of this policy are:

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- To guide staff, volunteers and governors in how to keep pupils safe online with regards to the curriculum and to internet filtering and monitoring.
- To help develop a culture of openness about life online and how to stay safe.
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

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 in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- 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.

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our academy funding agreement and articles of association.

3. Roles and Responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body 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 governing body 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 governing body will 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 lead (DSL).

The governing body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school 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 school's safeguarding needs

The governor who oversees online safety is Vikki Rundle-Brown, Safeguarding governor and Chair of Governors.

All governors will:

- Make sure they have read and understand this policy
- Agree to adhere to the terms of the ICT acceptable use policy relevant to their role
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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

The Head teacher

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

The Designated Safeguarding Lead (DSL)

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

The DSL takes lead responsibility for online safety in school. At Newcroft, the DSL is also the Head teacher. They:

- Make sure that staff understand this policy and that it is being implemented consistently throughout the school

- Work with the governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Provide governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Work with the ICT manager to make sure the appropriate systems and processes are in place
- Work with the Computing leader, ICTIC and other staff, as necessary, to address any online safety issues or incidents
- Manage all online safety issues and incidents in line with the school's safeguarding and child protection policy
- Respond to safeguarding concerns identified by filtering and monitoring
- Make sure that any online safety incidents are logged on CPOMS and actioned appropriately.
- Make sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online safety with the computing leader
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Trust or governing body
- Undertake annual risk assessments that consider and reflect the risks pupils face
- Provide 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.

The ICT manager

The ICT manager (ICTIC) with support of the school's Site Manager and Business Manager 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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

This list is not intended to be exhaustive.

All Staff and Governors

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

- 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 by alerting the DSL/ DDSL team without delay.
- Following the correct procedures by using staff filtering if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL/ DDSL team to make 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 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 are expected to:

- Notify a member of staff or the head teacher 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 ICT systems and internet (appendix 1)

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

Visitors, Volunteers and Members of the Community

Visitors, volunteers and members of the community who use the school's ICT systems or internet will use the guest filtering. They 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.

4. Educating Pupils About Online Safety

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

Pupils in **Key Stage 1** 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
- Use the school's 'stop, close, tell' approach to support them in keeping safe online both inside and outside of school
- Report concerns to a trusted adult without delay

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
- Be discerning in evaluating digital content

- Use the school's 'stop, close, tell' approach to support them in keeping safe online both inside and outside of school
- Report concerns to a trusted adult without delay

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online
- How to report concerns to CEOP, using the Report Abuse icon 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 with SEND.

5. Educating Parents and Carers about Online Safety

The school will raise parents/carers' awareness of internet safety through WEDUC letters and half termly newsletters which include a standing item about how to support their child with online safety and stay ahead of changes online.

The school will let parents and carers know:

- What systems the school uses to filter and monitor online use through the Online Safety Policy
- What their children are being asked to do online through curriculum documents published on the school's website and through parents' evening

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

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

6. Cyberbullying

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 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 encourage them 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. Class 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 PSHE, RSHE, Computing and any other subjects where appropriate.

The school also sends information on cyber-bullying in half termly newsletters to parents and 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 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 pupils, 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

More information can be found in the school’s Behaviour Policy.

Artificial intelligence (AI)

Newcroft Primary Academy recognises that AI has many uses to help pupils 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.

Newcroft Primary Academy will treat any use of AI to bully pupils seriously, in line with our Anti Bullying and Behaviour Policies.

Staff should be aware of the risks of using AI tools while they are still being developed. The school holds AI Risk Assessments. Any use of AI should be carried out in accordance with the Symphony Learning Trust AI Policy.

7. Acceptable Use

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT 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.

8. Pupil Mobile Phones in School

Pupils in Year 6 may bring their mobile phones to school to support their growing independence in walking to and from school. They are expected to turn them off and hand them to their class teacher where they will be stored until the end of the school day for pupils to collect on exit from the school site. Pupils of any age found with a mobile in their bag, or using a mobile in school during the day will be treated seriously and in line with the school's Behaviour Policy. More information can be found in the Behaviour Policy.

9. 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 using strong passwords and using 2 factor authentication where required by the Trust
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from any member of the school's senior leadership team, who will consult ICTIC and the school's site manager.

10. 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 Behaviour and ICT Acceptable Use policies. 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 Symphony Learning Trust Staff Disciplinary Procedures and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

Staff, Governors 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, half termly safeguarding newsletters 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 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

Governors 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.

Pupils

All pupils 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

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

12. Filtering and Monitoring at Newcroft

Filtering

- The overarching responsibility for filtering systems in school lies with the school's DSL.
- Staff, volunteers and governors understand their duty to keep children safe online using the school's internet.
- Staff and governors are trained annually at a minimum to understand their statutory duties regarding online filtering, how the school keeps children safe online through filtering and also how this is monitored.

- Volunteers are trained when they are inducted.
- Staff, volunteers and governors understand that the internet is continually changing, and that vigilance is key.
- School internet access is provided by Wave 9 and Sophos and includes filtering appropriate to the age of pupils.
- The school works in partnership with ICTIT to ensure systems to protect pupils are reviewed and improved.
- The school has 2 levels of filtering in place (a higher level for staff including social media for marketing of the school for teaching resources such as You Tube) to protect pupils. All pupil devices and any visitor devices are automatically set to pupil filtering levels and use a Guest log in.
- The school will perform regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.
- SENSO will flag potentially concerning content to DSL and DDSLs from pupil devices in real time, allowing for immediate action by the DSL team.

Monitoring of filtering

- If staff or pupils come across unsuitable online materials, the it must be reported to the DSL/ DDSL team, which is investigated immediately and the device removed.
- Should there be a breach, appropriate action is taken to log the breach on the school's online log, to be actioned by the DSL team and IT team.
- Should a pupil be found to be searching for inappropriate materials in school, parents would be informed by the DSL, support and education offered to both parents and the pupil, and a log be made on the child's CPOMS safeguarding record.
- The DSL and IT team receive a weekly filtering log check and action anything suspicious or concerning with ICTIC. They action this to ensure that such materials can no longer be accessed.
- The school engages in regular external filtering testing using the KCSIE recommended SWGFL Test Filtering and obtains a certificate of evidence.
- The school completes an Internet Filtering and Monitoring Standards for Schools and Colleges Check/ Review on an annual basis to ensure the school meets its statutory duties.
- The DSL/DDSL team will review flagged content and act accordingly following safeguarding procedures.
- Governors understand their statutory duty to monitor filtering. The safeguarding governor checks the school's logs on a termly basis and as part of the annual safeguarding audit.

13. Monitoring Arrangements

The DSL/ DDSL team and teachers log behaviour and safeguarding issues related to online safety on CPOMS.

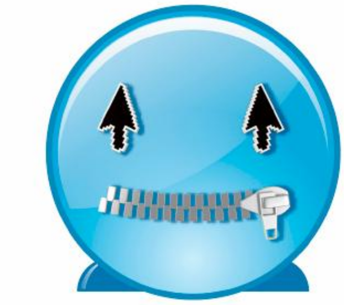
This policy will be reviewed every year by Head teacher/ DSL/. At every review, the policy will be shared with the governing board.

Appendix 1

Pupil IT Acceptable Use Policy

Please **complete all shaded boxes**

To keep myself safe whilst I use technology, I will…

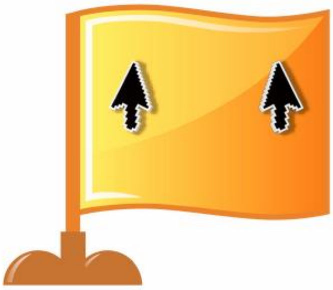


ZIP IT

Keep my personal information private and think about what I say and do online.

BLOCK IT

Block people who send unkind messages and don't open unknown links and attachments.



FLAG IT

Flag up with a trusted adult if anything upsets me or if a stranger contacts me.

Using school technology

- ✓ I will follow the Rainbow Rules.
- ✓ I will be kind and respectful to others online.
- ✓ I will keep my username and password private and never use anyone else's.
- ✓ I will keep my personal information private.
- ✓ I will ask for permission before using school technology.
- ✓ I will use school technology sensibly and responsibly.
- ✓ I will only use programs, apps and websites that I have permission for.
- ✓ I will avoid unsuitable, unsafe or illegal content.
- ✓ I will ask for permission before accessing anyone else's files or information.
- ✓ I will ask for permission before taking or sharing pictures or videos of others.
- ✓ I will respect the work of others and ask for permission before using it.
- ✓ I will use 'stop, close, tell' if I see something that worries or upsets me.

I have read and understand this policy and agree to follow it.

Pupil name	Pupil signature

I have read and discussed this policy with my child and give permission for them to use the school's IT systems, including the internet.

Parent/Carer name	Parent/Carer signature	Date

Please notify the school office of any changes to these arrangements