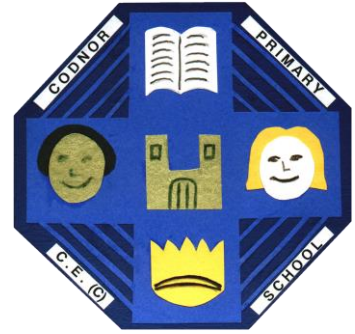


Codnor Community Primary School



Online Safety Policy

September 2025

Mr James Blake
Headteacher

CODNOR COMMUNITY PRIMARY SCHOOL

Policy for Online Safety

Introduction

Codnor Community Primary School fully recognises its responsibilities regarding Child Protection and Safeguarding. This Online Safety policy sets out how the school will deliver these responsibilities in addition to the Child Protection and Safeguarding Policy, and Acceptable Use of IT Policy.

This policy should be read alongside the school's behaviour policy, anti-bullying policy, and AI policy.

Aims

Our school aims 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.

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.
- **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 the following advice and legislation:

- [Working Together to Safeguard Children](#)
- [Preventing and tackling bullying](#)
- [Searching, screening and confiscation in schools](#)
- [The Prevent duty: safeguarding learners vulnerable to radicalisation](#)
- [Derby City & Derbyshire Safeguarding Children Board procedures](#)
- [Education Act 1996](#)
- [Education and Inspections Act 2006](#)
- [Education Act 2011 Part 2 \(Discipline\)](#)
- [Health and Safety at Work etc. Act 1974](#)
- [Obscene Publications Act 1959](#)
- [Children Act 1989](#)
- [Human Rights Act 1998](#)
- [Computer Misuse Act 1990](#)

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.

Roles and responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school. These sections are not intended to be exhaustive.

The governing body has overall responsibility for monitoring this policy and ensuring its implementation.

The governing body will ensure that 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 ensure that 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, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. This includes:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions, including receiving anonymised reports of online safety incidents and statistics regarding attempted access to blocked sites, through meetings with a Designated Safeguarding Lead (DSL). Where this role is delegated to the safeguarding governor, the governor reports this information to the governing body.
- Checking that staff training is taking place as intended.
- Having effective filtering, monitoring and recording systems in place that meet school's safeguarding needs; and that harmful and inappropriate content is blocked, without unreasonably impacting teaching and learning.

All governors will:

- Ensure 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).
- 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

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

Designated Safeguarding Leads (DSLs) take 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 and reviewed regularly, and as necessary.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager/third party supplier to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager/third party supplier and other staff, as appropriate, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Ensuring that any online safety/cyber-bullying incidents are logged and dealt with appropriately in line with this policy and the behaviour policy.
- Liaising with other agencies and/or external services if necessary.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety training, to all staff in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Meet with the governing body/safeguarding governor to discuss current issues, review anonymised incidents and filtering and monitoring logs, and ensure that annual (at least) filtering and monitoring checks are carried out.

The ICT manager/third party supplier 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 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.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff are responsible for:

- Maintaining an understanding of this policy as a core part of safeguarding and implementing it consistently; and having an awareness of current online safety matters/trends and basic cybersecurity.

- Maintaining a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the Internet (appendix), including safe use of passwords; and ensuring that pupils follow the school's terms on acceptable use (appendix).
- Supervising and monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- Following all relevant guidance and legislation, e.g. Keeping Children Safe in Education and UK GDPR regulations.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any failures of those systems/processes by speaking directly to a DSL.
- Speaking to a DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with DSLs to ensure that any online safety or cyber-bullying incidents are logged (see Monitoring Arrangements below) and dealt with appropriately in line with this policy and the school's behaviour policy; and adopting a zero-tolerance approach to incidents of sexual harassment/violence, harassment, discrimination, hatred, etc. – maintaining the notion that 'it could happen here'.
- Immediately reporting any suspected misuse or problem to the headteacher, a member of the SLT, or a DSL for investigation/action, in line with the school safeguarding procedures.
- Maintaining an awareness of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, and prioritising human oversight: AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact and sense-checked and critically evaluated (in line with school's AI policy).
- Ensuring that all digital communications with learners, parents and carers, and others are on a professional level and only carried out using official school systems (e.g. school email addresses).
- Modelling safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media, and follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.

Learners are responsible for:

- Using the school's systems in accordance with the Acceptable Use terms (appendix 1 and 2).
- Reporting misuse of the school's systems to a member of staff.
- Speaking with a member of staff if they or someone they know feels vulnerable when using online technology.

- Understanding the importance of adopting good online safety practice when using digital technologies out of school.

Parents/carers 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).
- Seek further guidance on keeping children safe online and maintain vigilance when children are using internet-connected devices.

Online safety within the curriculum

Pupils are taught about online safety as part of the curriculum. We use the Purple Mash Computing Scheme of Work which has '2BeSafe' online safety units, designed to be taught flexibly. These 15-minute lessons can be taught as part of Computing, PSHE, RSE, or as a response to an online safety issue/incident. The lessons are progressive through each year group. The aim is to give all pupils the underpinning knowledge of aspects of the online world to help them develop behaviours that can help them navigate safely and confidently regardless of the device platforms or apps they are using. It also aims to help pupils develop appropriate scepticism and reasoning when they encounter new online experiences to be able to evaluate the risks or potential pitfalls of these encounters.

We supplement this teaching with whole-school online safety awareness and through role modelling in the day-to-day life of the school.

Online safety teaching is appropriate to pupils' ages and developmental stages as well as being flexible enough to be tailored to any specific emerging threat within the community.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Health, wellbeing and lifestyle
- Privacy and security
- Managing online information
- Copyright and ownership

When teaching aspects of online safety, teachers review external resources prior to their use to ensure they are appropriate and a valid source of information, and report any unsuitable material to the headteacher, a member of the SLT, or a DSL. Teachers are sensitive to the topic being covered and the potential that pupils may have suffered/be suffering from online abuse or harm in this way.

If teachers have any concerns, they must consult with a DSL, who will advise on how best to support pupils who may be especially impacted by a lesson or activity. Lessons and activities are planned so they do not draw attention to individual pupils who may be experiencing difficult circumstances. If a staff member is concerned about anything pupils raise, they will make a report on MyConcern in line with the safeguarding policy.

Informing parents/carers about online safety

The school will raise parents/carers' awareness of Internet safety via the school website. This policy will also be shared with parents/carers. The school will let parents/carers know what systems the school uses to filter and monitor online use.

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.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We 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 actively discusses cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health and Citizenship Education (PSHCE), and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school website helps keep parents/carers up to date on what bullying and cyber-bullying look like, and how school deals with incidents.

In relation to a specific incident of cyber-bullying, the school follows 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.

A 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.

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 and staff. If the search is not urgent, they will seek advice from the headteacher, a member of the SLT and/or a DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil'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 staff member in conjunction with the headteacher, a member of the SLT, and/or a 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 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/carers 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 headteacher, a member of the SLT, and/or a DSL immediately, who will decide what to do next. The decision will be made 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 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](#)
- School's behaviour policy.

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

Children's mobile devices in school

There are legitimate reasons for some pupils bringing devices into school. Children who walk to/from school on their own, for example, can carry a phone to help ensure their safety on the streets. If pupils bring mobile phones or smart watches to school, their devices must be switched off and taken to the office, to be collected at the end of the day – not kept in pupils' bags. School cannot be held responsible for any loss of, nor damage to, these devices. School takes precautions to secure them while they are in school, but they are stored strictly at their owner's risk.

Some parents have specified that they do not want their child to appear on social media. Therefore, during after-school events (e.g. school discos), school does not allow pupils to use any technology from home which has the capability to record. If pupils bring devices to these events, they must be stored as above.

School does support parents who want to make recordings of events such as nativities and sports days, as these are memories of their children growing up, but this is on the understanding that these recordings are only for parents' personal use and are not shared publicly on social media in any form, and that parents are responsible for keeping these recordings private.

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.

Staff using work devices outside school

A local user logon is provided as the only user account which can be used when not connected to the school network. The local user logon allows the user to select their own wireless network. The local user logon is subject to the same restrictions as the other user accounts in the school.

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

Staff members must enable the device to install updates when prompted.

Responding to issues of misuse

Where a pupil misuses the school's ICT systems or Internet, we will follow the procedures set out in school's behaviour policy and anti-bullying policy. 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 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.

Training

Staff receive training in online safety, Prevent and cyber-bullying in line with our Safeguarding CPD schedule. New members of staff are trained on school's filtering/monitoring systems as part of their induction. DSLs will undertake child protection and safeguarding training, which will include online safety, every 2 years. Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training.

Monitoring arrangements

Alerts from the filtering/monitoring system are automatically sent to the safeguarding@ address. DSLs and the headteacher have access to this.

Behaviour and safeguarding issues related to online safety are logged on MyConcern. The following information is logged:

- Date and time
- Where the incident took place

- Description of the incident
- Action taken
- Name of the staff member(s) recording the incident.

Monitoring and evaluation

The Headteacher is responsible for the review, monitoring and evaluation of the Policy in consultation with the rest of the staff.

Policy review

A review of the Policy will take place in line with the School Improvement Plan.

Governor approval

Any amendments to the Policy will be presented to the Governors for approval at the next available meeting.

Mr J. Blake
Headteacher
September 2025

Appendix

EYFS and KS1 acceptable use (PowerPoint presentation in Staff Area) to use with children.

Here are the rules for using computers and other electronics in school.

- Ask a teacher or adult before using them.
- Only use websites that a teacher or adult has told me or allowed me to use.
- Tell my teacher immediately if:
 - I visit a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends.
- Use school computers for school work only.
- Be kind to others and not upset or be rude to them.
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my hardest to remember my username and password.
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
- Save my work on the school network.
- Check with my teacher before I print anything.
- Log off or shut down a computer when I have finished using it.

I know that school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

KS2 acceptable use (PowerPoint presentation in Staff Area) to use with children.

Here are the rules for using computers and other electronics in school.

- Always use the school's ICT systems and the internet responsibly and for educational reasons only.
- Only use them with a teacher's permission.
- Keep my usernames and passwords safe and not share these with others.
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find anything that might upset, distress or harm me or others, or if I see other people finding – or even just searching for something like this.
- Always log off or shut down a computer when I've finished working on it.
- If I bring a mobile phone into school, I will switch it off and take it to the office, to be collected at the end of the school day.

I will not:

- Access any inappropriate websites, including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate.
- Log in to the school's network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

I know that school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Staff acceptable use (emailed out)

When using the school's ICT systems and accessing the Internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way that could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Take photographs of pupils without checking whether they are allowed to be in the public domain (e.g. for the school website).
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let a DSL and the ICT Manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and Internet responsibly, and ensure that pupils in my care do so too.

Use of the school's ICT systems constitutes the staff member's agreement to the Acceptable Use Policy.