Achieving Believing Caring Sharing

NORTH CAVE
C of E PRIMARY
SCHOOL

Online Safety Policy

September 21

School vision:

A Christian school at the heart of the community that we serve.

Achieving our goals as we are guided by God’s light.

Believing in ourselves, in each other and in God.

Caring and nurturing all of God’s children in our school family.

Sharing our aspirations through our exciting, enriched and inclusive curriculum.

‘Therefore encourage one another and build each other up, just as in fact you are doing.’ 1 Thessalonians 5 Verse 11

Achieving Believing Caring Sharing

NORTH CAVE
C of E PRIMARY
SCHOOL

Train up a child in the way he should go; even when he is old he will not depart from it.

Proverbs 22:6

Introduction

The use of technology continues to be an important component of safeguarding young people. Technology, whilst providing many opportunities for learning also provides a platform that can facilitate harm. Keeping Children Safe in Education categorises online safety into three broad areas:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

It is with these three categories in mind that this policy outlines the roles, responsibilities and procedures for ensuring online safety.

Aims

This policy aims to set out the school's position in how it will strive to provide a safe environment for all of the school community whilst using ICT within the school, and how it will also strive to ensure that its members also use ICT, including their own personal devices, in a safe and responsible manner whilst outside of the school grounds.

This policy will detail the individual responsibilities of each of the key people in the school who have a role to play in fulfilling this policy and its related procedures.

This policy applies to all staff, children, governors and parents of the school community. It should be read in conjunction with the supporting policies and related information that is detailed below.

North Cave CE Primary School believes that ICT can and should be used to enrich the education of all children. ICT also provides the staff of the school with a great many tools to help them play their part in providing the children of the school their education. Whilst the school sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The school believes that online safety is the responsibility of the whole school community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

Social Networking is becoming an increasingly popular tool within our environment to support learning, encourage creative and appropriate use of the internet and to publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged. We also expect staff to maintain a professional level of conduct in their use of these types of technologies.

Risks & Responsibilities

Risks of ICT use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of the internet and ICT
- Exposure to age inappropriate materials
- Inappropriate or illegal behaviour
- Consensual and non-consensual sharing of inappropriate content and images
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users
- Inappropriate or illegal behaviour by school staff
- Actions that bring the school into disrepute
- Online grooming or child exploitation

Creating a Safe ICT Learning Environment

The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of **whole-school awareness**, **designated responsibilities**, **policies and procedures**. This is achieved by:
    - Raising awareness of the risks of ever-changing technology that is both emerging and already embedded in the school community.
    - Ensuring that the Online Safety policy and education programme adapt to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to Online Safety.
    - Ensuring that the school's policies and procedures are effective and kept up to date, and also make clear to all members of the school community what is acceptable when using ICT and the internet.
2. Make use of **effective technological tools** to ensure the safe use of the internet and school ICT systems. These include:
    - Firewall protection to the school's network.
    - Virus protection of all relevant IT equipment connected to the school's network.
    - Filtering, logging and content control of the school's internet connection.
    - Monitoring systems.
3. Develop an **Online Safety education programme** for the whole school. This will consist of:

[1] This list is by no means exhaustive, but means to highlight some of the main areas of risk that the school has identified.

- An on-going education programme for the children at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
- Continued Professional Development for staff to ensure that they are equipped to support the children at the school, and are also fully aware of their responsibilities in using ICT, both in and out of the school.
- An on-going education programme for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the school in these matters.
- Explaining how accessing and / or sharing other people’s personal information or photographs might be inappropriate or illegal.
- Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.

Headteacher’s Responsibilities

1. To take ultimate responsibility for online safety whilst delegating the day-to-day responsibility to the Online Safety Coordinator (OSC).
2. To ensure that the OSC is given enough time, support and authority to carry out their remit.
3. To ensure that the local governing body is kept informed of the issues and policies.
4. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the online safety programme.

Governing Body's Responsibilities

1. To ensure the Designated Safeguarding Governor considers online safety as a part of the regular review of child protection and safeguarding.
2. To support the Headteacher and OSC to ensure that the correct policies and procedures are in place, and also that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of online safety to parents.

Online Safety Coordinator's Responsibilities

1. To develop and review the appropriate online safety policies and procedures.
2. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
3. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of online safety inside and outside of the school environment.
4. To work with the appropriate members of staff to develop an online safety education programme for the children.

5. To work with the appropriate members of staff to develop a parental awareness programme for online safety at home.
6. To maintain a log of all online safety incidents that occur in the school.
7. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
8. To meet with the Designated Safeguarding Lead regularly to discuss online safety and progress.
9. To liaise with any outside agencies as appropriate.
10. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Designated Safeguarding Lead's Responsibilities

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
2. To liaise with the OSC on specific incidents of misuse.
3. Take a proactive role in the online safety education of the school's children.
4. Develop systems and procedures for supporting and referring children identified as victims or perpetrators of online safety incidents.
5. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

IT Support Staff Responsibilities

1. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the OSC, Headteacher and Police if necessary.
2. Review the technological systems upon any discovery or breach of the Acceptable Use Policy (AUP), to ensure that the same breach does not happen again.
3. Liaise with the school if any breach can be traced back to an individual child.
4. Liaise with the OSC and Headteacher if any breach can be traced back to an individual member of staff.
5. Provide the technological infrastructure to support the online safety policies and procedures.
6. Report any network breaches of the school's Acceptable Use Policy or Online Safety Policy to the OSC.
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Special Educational Needs Coordinator's Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard as to how they may affect children and young people with additional educational needs.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Classroom Teachers, Teaching Assistants and Site Staff Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard to how they might affect children and young people.
2. To implement school online safety policies through effective classroom practice.
3. To ensure any incidents of ICT misuse are reported through the correct channels.
4. To ensure that the necessary support is provided to students who experience problems when using the internet, and that issues are correctly reported to the OSC.
5. To plan classroom use of ICT facilities so that online safety is not compromised.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Children's Responsibilities

1. To uphold all school online safety and ICT policies.
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they, or another child experience problems online.
4. To communicate with their parents or carers about online safety issues and to uphold any rules regarding online safety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting online safety
2. To discuss online safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the school.

Procedures & Implementation

The school, through the Online Safety Coordinator, will ensure that all staff are aware of the policies and procedures being implemented to meet the Online Safety remit. There will be information available to all staff about the technologies that are already in use at the school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the school's online safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

Online safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and courses of action.

Children

The students at the school will be made aware that there is a whole school approach to online safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Children will be invited to participate in the future planning and discussions regarding online safety and their opinions will be regularly gauged as to the effectiveness of the provision.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that North Cave CE Primary School is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

Parental workshops will be delivered to give parents the opportunity to understand online safety topics and new risks children are exposed to.

Firewall

The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

The responsibility lies with the IT support staff for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Monitoring Systems

The school/Trust has many different monitoring system at its disposal including:-

- All files stored on the school's servers can be searched and checked
- Teachers can monitor the pupils' use of computers
- Any incident that has a consequence attached to it is entered into the school's behaviour logging system.

Where incidents raise concern regarding a child's welfare they will be also recorded on our online Child Protection Monitoring System CPOMS where a pattern of concern can be identified if appropriate.

Currently, school-owned iPads are filtered through the web proxy with the most restrictive policy applied.

Online Safety Education

All children at the school will receive an on-going online safety education programme.

This programme will inform the children of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The School's PSHE curriculum is under constant review to include emerging trends in children's online use and to address new uses as they arise.

The school will follow the Safer Internet Day programme and deliver those resources through collective worship. Teachers will be informed about the content being delivered, and asked to discuss the content after the assembly is given so that students have an opportunity to raise any concerns or issues from this information.

The PSHE and Personal Development curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.

The SENCO will work with the OSC to ensure that there are accessible and adequate resources available for SEND students of the school to access the same online safety education as the rest of the school.

Responding to a concern

Appendix 1 outlines the process regarding concerns being raised relating to online safety.

As a school, we proactively work to ensure the safety of our children both in-school and online. We do not have the capacity to police all online activity outside of school, however where actions of a child online go against the school's Behaviour Policy, we will address these concerns directly.

Where actions taken by students online pose a risk to them or others, they will be dealt with in line with our Child Protection Procedure, conducting appropriate risk assessments and ensuring minimal disruption to any victim, where appropriate.

Consistent Approach

The OSC will ensure there is a commonality of approach in responding to online safety incidents and that the correct reaction and procedure is followed by all staff when dealing with an online safety issue.

School Social Media Accounts

The school hosts a social media account.

Whilst all social media is different, and constantly evolving there are some key expectations for colleagues using social media in school, which are as follows:

- All social media must be set up to ensure that that there can be no private communication or Direct Messaging between the account and the accounts of students.
- Passwords should not be shared between colleagues and one colleague should take overall responsibility for the account and its content.
- Users should follow the expectations and responsibilities of colleagues outlined above.

As stated above, social media is constantly changing and as such advice should be sought from the OSC where appropriate.

Supporting Policies and Related Information

North Cave CE Primary School/Education Alliance supporting policies:

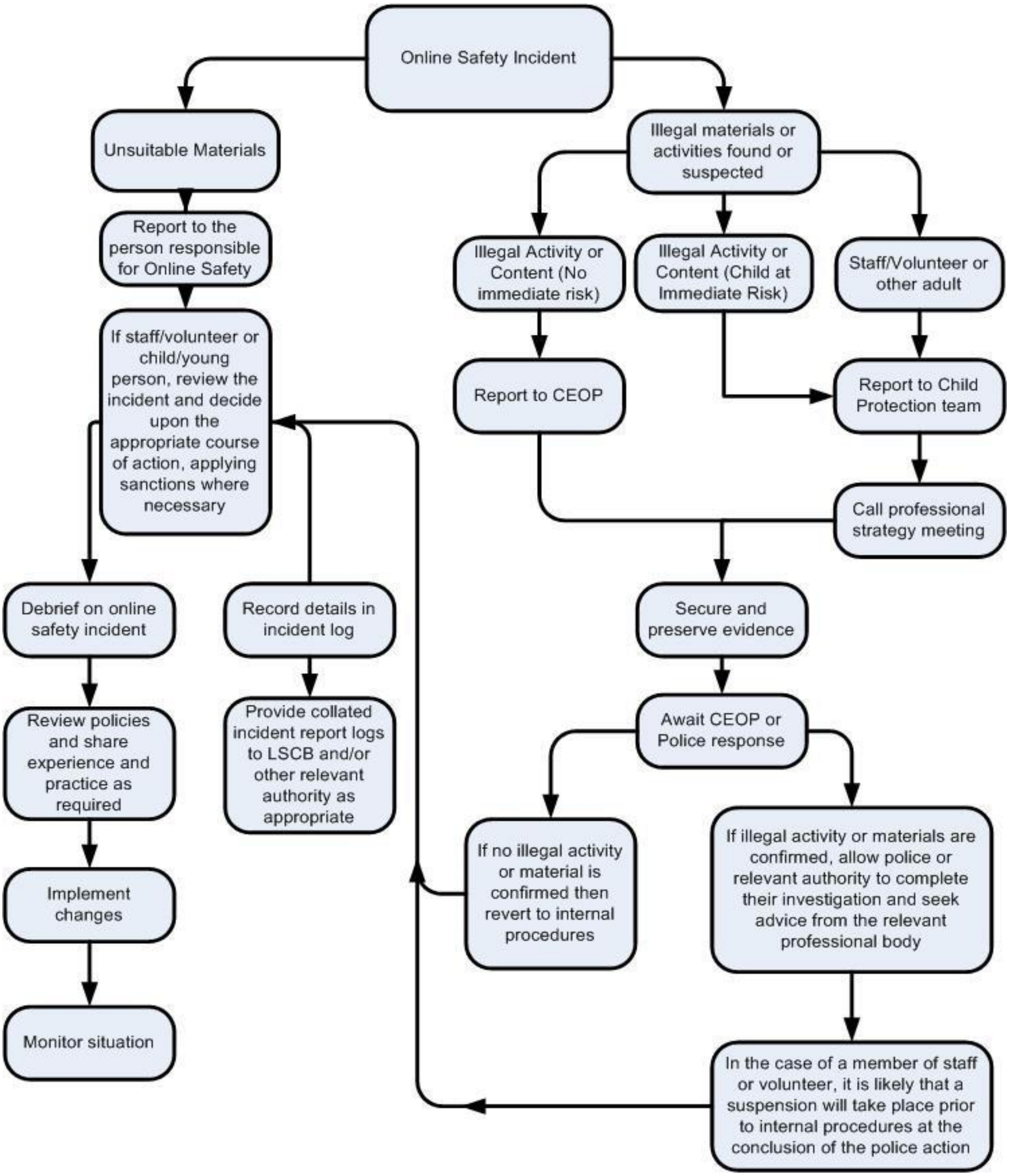
- Child Protection Policy & Procedure
- Expectations and Code of Conduct for Staff
- Prevent Policy
- Behaviour Policy

- **Procedure for Policy Implementation**

The procedural document for this policy is attached as an appendix.

- Appendix 1 – Online Safety Incident Reporting Flowchart

Appendix 1 - Responding to incidents of misuse (Flow Chart)



Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action