CHRIST CHURCH C.E. FIRST SCHOOL

-Online Safety Policy-

Headteacher: Mrs A Graham

Chair of Governors: Mr M Bird

Policy Agreed: February 2024

Review date: February 2026

Christ Church C.E. First School
Northesk Street, Stone
Staffordshire, ST15 8EP
Tel: 01785 336545
Company registration Number: 07702211
Email: office@christchurch-stone.staffs.sch.uk
Website: http://www.christchurch-stone.staffs.sch.uk

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Leader
- Staff – including senior leaders, teachers, support staff
- Governors/Board
- Parents and carers

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*March 2020*
The implementation of this online safety policy will be monitored by the:	*A Richardson*
Monitoring will take place at regular intervals:	*Annually*
The Local Governing Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*March 2021*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, Academy CEO, Trust Board, LADO, Police*

This policy applies to all members of the school community who have access to and are users of school digital technology systems, both in and out of the school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors-

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors. They will receive regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of 'Online Safety Governor'.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

Online Safety Lead

- Leads online safety within the school
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Liaises with the LA/ MAT/ Headteacher/ Link Governor/ Technical staff/ Members of school staff (i.e. to provide regular training/ updates)
- Attends relevant meetings with Governors/ senior leaders

Network Manager/Technical staff

- That the school's technical infrastructure is secure and that the school meets required online safety requirements.
- The filtering policy is applied and updated on a regular basis
- That the use of the networks/internet/digital technologies is regularly monitored to ensure that any misuse/attempted misuse can be reported to the Headteacher and Online Safety Lead for investigation.
- That monitoring of software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the staff acceptable use policy/agreement
- They report any suspected misuse or problems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies which are relevant to their age and stage. (EYFS&KS1/ KS2)
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

Pupils

All Pupils, including children in EYFS will be taught about online safety and online-bullying as part of the curriculum. Teaching staff follow a scheme of work to ensure that they are teaching the children to be responsible digital citizens.

In Key Stage 1, pupils will be taught to:

- Use a range of technology safely, respectfully and responsibly keeping personal information private, in accordance with the pupil acceptable use agreement.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use a range of technology safely, respectfully and responsibly keeping personal information private, in accordance with the pupil acceptable use agreement.
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- How to report a range of concerns
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (in line with their age)

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use internet/technology devices in an appropriate way both inside and outside of school. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practices. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher or Online Safety Lead.

Policy Statements

Education –Pupils

The education of pupils in online safety/digital literacy is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided for all pupils in all year groups (Reception-Y4) as part of Computing/RSE/other lessons.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils are encouraged in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Pupils are supported to understand the need for the pupil acceptable use agreement and are encouraged to adopt safe and responsible use both within and outside school.
- All members of staff will act as good role models in their use of digital technologies and the internet in lessons where internet use is pre-planned. It is best practice that pupils should be guided to sites checked

as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. A planned programme of formal online safety training will be made available to staff, including new members of staff. The Headteacher and Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. This policy will be monitored and reviewed regularly.

Governors should take part in regular online safety training/awareness sessions.

Technologies- Pupils

-Pupils are not allowed to bring personal/ technology devices into school.

-Pupils are not allowed to access any messaging apps/ social media/ blogs during school time on any of the school's technology devices.

Technologies- Staff

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice.

The school allows staff to bring in their own personal devices. However, the use of mobile phones in classrooms or public places around school is not allowed when children are on the premises. All mobile phones must be stored securely out of reach within the setting during contact time with children. In EYFS (Early Years Foundation Stage) phones are kept in a locked cabinet whilst the children are in school.

Use of digital videos and images

Please refer to the whole school policy for the use of mobile phones, cameras and devices.

Communications

When using communication technologies, the school considers the following as good practice:

- Official school email services are regarded as safe and secure and they are monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to a member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school's website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All settings have a duty of care to provide a safe learning environment for pupils and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

All staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Dealing and responding to incidents of misuse

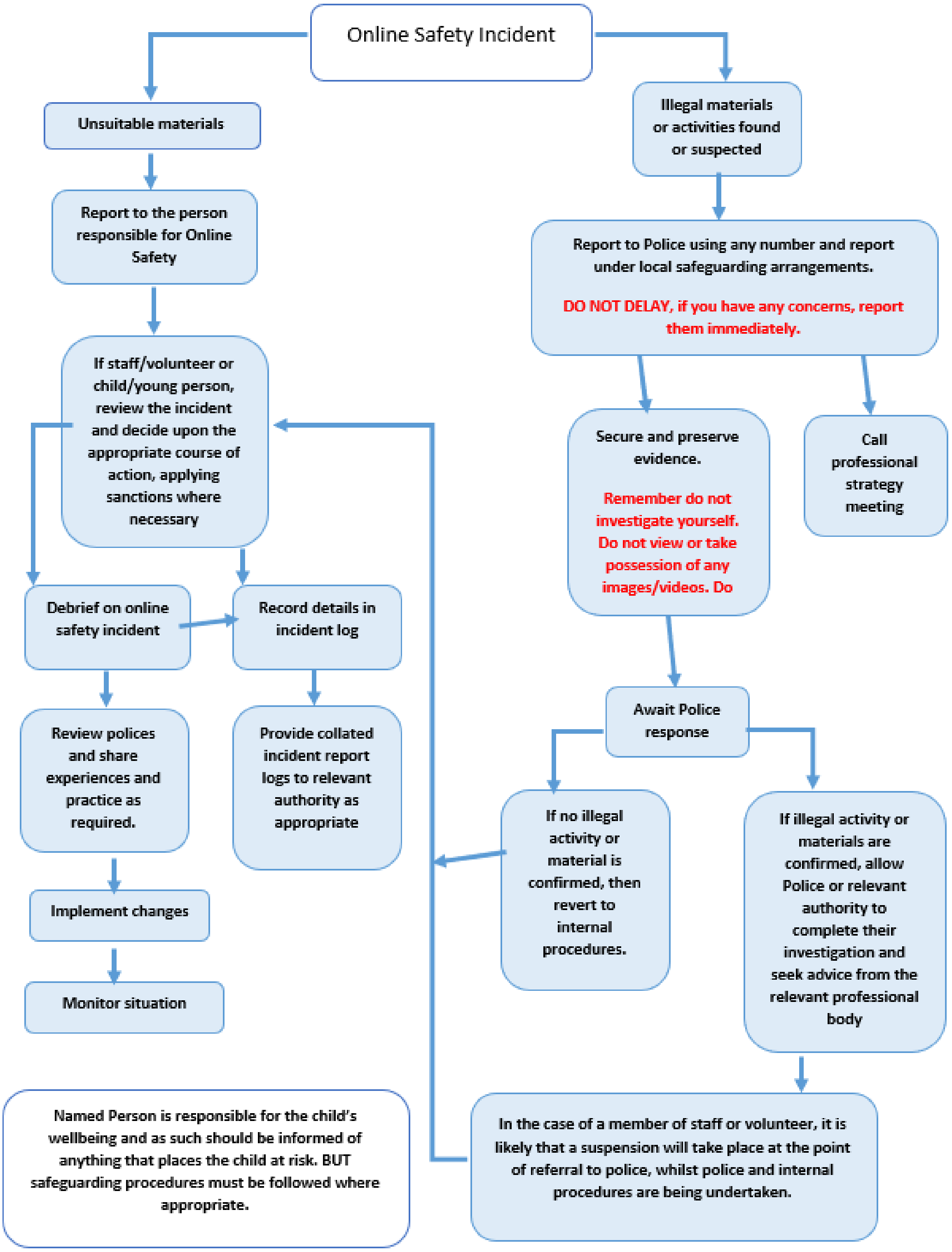
- Complaints of Internet misuse will be dealt with by the Headteacher and Online Safety Lead

- Any complaint about staff misuse must be referred to the headteacher.

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in the school context, either because of the age of the users or the nature of those activities.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

The 'Online Safety Incident' guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await 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

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.