Christ the King Catholic Academy and St Cuthbert's Catholic Academy

Care - Courtesy - Concern

Online Safety Policy

January 2024

Effective date: January 2024
Version 1.1
Blessed Edward Bamber Catholic Multi Academy Trust

E-Safety Policy

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE) and other statutory documents; it sits alongside the school's statutory Safeguarding and Child Protection Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Introduction

Christ the King and St Cuthbert's Catholic Academy will undertake to ensure compliance with the relevant legislation with regard to the provision of e-safety. This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Christ the King and St Cuthbert's Catholic Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

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.

We have a named e-safety leader, who is the ICT Lead,); this person is not the designated safeguarding lead (DSL), but KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." The DSL and ICT Lead work together to ensure online safety is adhered to. When incidents of online safety are brought to the school's notice, both the DSL and ICT Lead agree an appropriate way forward in-line with procedures outlined in both the CP Policy and E-Safety Policy.

(Executive) Headteacher

The (Executive) Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the ICT Lead. They and (at least) another member of the senior leadership team 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 (Executive) Headteacher /senior leaders are responsible for ensuring that the ICT Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant. They 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.

All staff

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and ICT Lead are
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Notify the Executive Headteacher/DSL/ICT Lead if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise
- Whenever overseeing the use of technology in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils/students to follow their acceptable use agreement, remind them about it and enforce school sanctions
- Take a zero-tolerance approach to bullying and sexual harassment even if appears to be low-level (the DSL will update staff of the latest guidance from the DfE)
- Be aware that you may see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – All incidents must be reported on MyConcern or reported to the DSL
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in the ICT Acceptable Use Policy, Staff Handbook and The Code of Conduct for Employees

PSHE Leader

In addition to the staff responsibilities, they must include mental wellbeing, healthy relationships and staying safe online into the PSHE curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."

Computing Curriculum Leader
In addition to the staff responsibilities, they must oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum. They must work closely with the DSL/PSHE Lead and all other staff to ensure an understanding of the issues, approaches and messaging, collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. Staff in the first instance will report using the MyConcern reporting system
- reports will be dealt with as soon as is practically possible once they are received. Senior staff members and the ICT Lead receive instant notifications via email if any safeguarding breaches have been met by the school Smoothwall protection system.
- the Designated Safeguarding Lead, ICT Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures and acted upon urgently.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the CEO of the Blessed Edward Bamber Catholic Multi Academy Trust

Proceedures
Incidents should be logged regardless of the substance of the complaint or findings.

Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

Filtering
The school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours. The school manages access to content across its systems for all users. The school uses Smoothwall as an externally provided filtering service.

Access to online content and services is managed for all users.

There are established and effective routes for users to report inappropriate content which has not been detected.

There is a clear process in place to deal with requests for filtering changes, which is led by the ICT Lead
The school provides enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)

Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
Where personal mobile devices (Staff only) have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring
The DfE guidance "Keeping Children Safe in Education" states:
"It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. "

The school has monitoring systems in place to protect the school, systems and users. The school monitors all network use across all its devices and services. An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

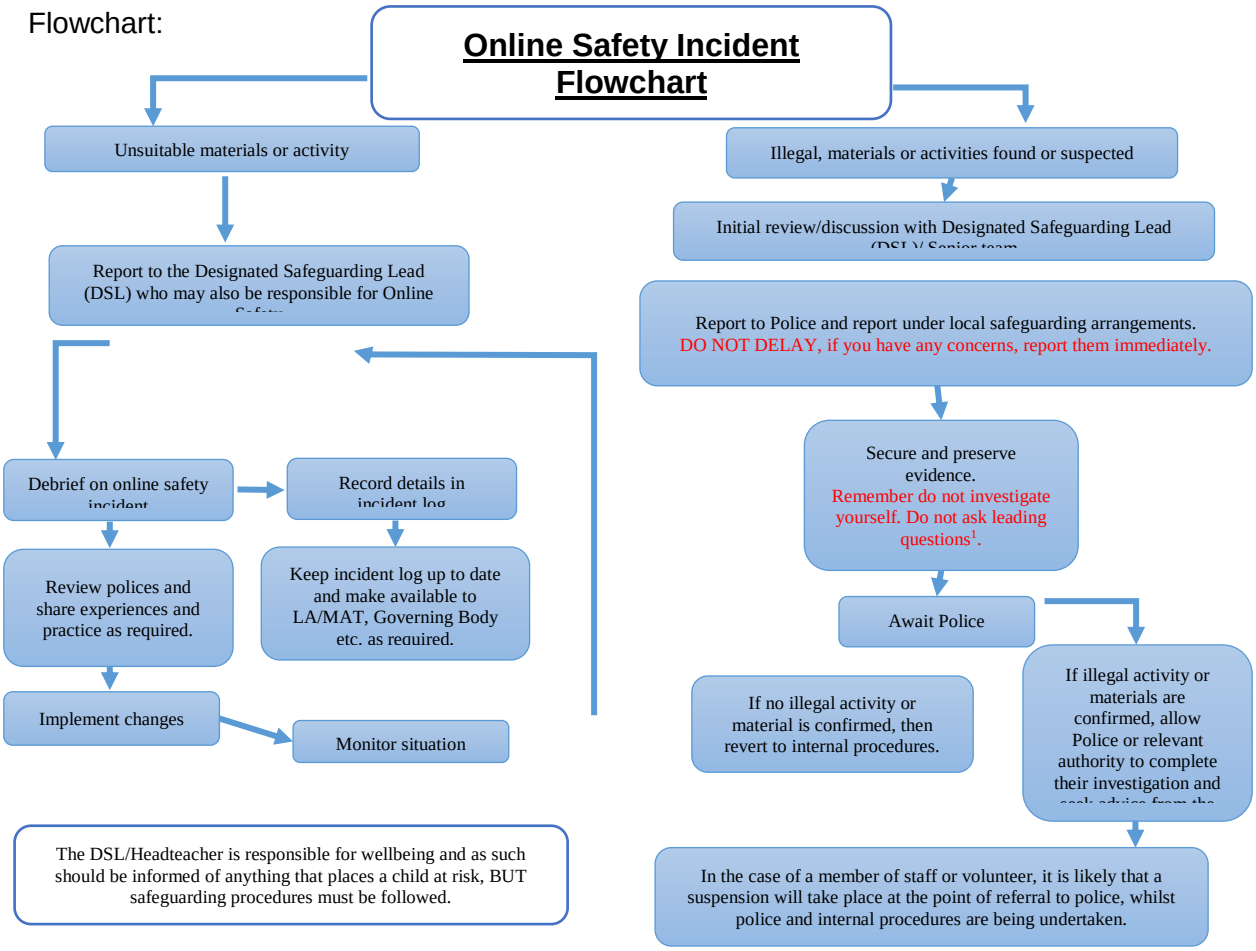
Monitoring includes:
- physical monitoring (adult supervision in the classroom)
- filtering logs are regularly analysed and breaches are reported to senior leaders and ICT Lead
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to senior leaders and ICT Lead

Technical Security
The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines copies off-site or in the cloud
- all users have clearly defined access rights to school technical systems and devices.

Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the ICT lead

- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by ICT Lead / External IT service provider who will keep an up-to-date record of users and their usernames
- the master account passwords for the school systems are kept in an online secure place and managed by competent members of the technical team
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for younger learners may be reduced
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- ICT Lead / External Technical service provider is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- staff are restricted from downloading executable files and installing programmes on school devices
- BitLocker system is used regarding the use of removable media (e.g., memory sticks/USB storage) by users on school devices.

Flowchart:


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online
Debrief on online safety
Record details in
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
Illegal, materials or activities found or suspected
Initial review/discussion with Designated Safeguarding Lead
Report to Police 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 ask leading questions[1].
Await Police
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
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.