NAVENBY CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY POLICY

This policy was approved by Governors on 20th November 2025 and is reviewed annually.

This policy applies to all members of the Navenby School community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to or are users of school technology systems, both in and out of the school.

School Roles

The role of the ICT Governor will include:

- meetings with the ICT subject leader to monitor online safety incidents and curriculum coverage regarding online safety
- receiving any updates from the school's Designated Safeguarding Leaders (DSL) regarding incidents flagged by the school's Smoothwall system

The role of the Headteacher will include:

- The Headteacher has a duty of care for ensuring the safety, including online safety, of members of the school community, though the day-to-day responsibility for online safety will be delegated to the school's ICT leader (S. Sheardown)
- that staff have read and understood the Staff Code of Conduct Policy section 7.3 regarding e-safety as part of their induction process

The role of the ICT & E-Safety School lead:

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that a clear and progressive e-safety curriculum is in place for all children
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- receives reports of online safety incidents from school staff and/or Smoothwall and keeps a log of incidents to inform future online safety developments
- meets with the ICT Governor to discuss any e-safety issues & review curriculum coverage
- reports regularly to other members of the Senior Leadership Team regarding e-safety

The role of the Network Manager (F1 Group, sent a copy of this policy) ensures:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through properly enforced password protection and encrypted devices
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the school's e-safety lead and/or e-safety governor for investigation
- that monitoring software / systems are implemented and updated regularly

The Role of Teaching & Support Staff ensures:

- they have an up-to-date awareness of online safety and of current school practices
- they have read and understood the Staff Code of Conduct Policy
- they report any suspected misuse or problems to the school's ICT lead for investigation
- all digital communications with pupils or parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Internet Safety Pledge
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of technology in lessons and other school activities
- 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

The role of the School Designated Safeguarding Lead (F. Reeder) & Data Protection Officer (S. Sheardown):

These individuals 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
- cyberbullying

The role of the pupils:

- to be responsible for using school ICT equipment with respect and care
- to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (KS2)
- to understand the importance of reporting abuse or access to inappropriate materials and know how to do so
- to understand the importance of online safety practices when using technology out of school

The role of the parents/carers:

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website updates and literature relating to digital parenting.

School Computing Equipment

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All pupils will be provided with a username and password
- All pupils will have secure access to Google Classroom to access any remote learning if needed

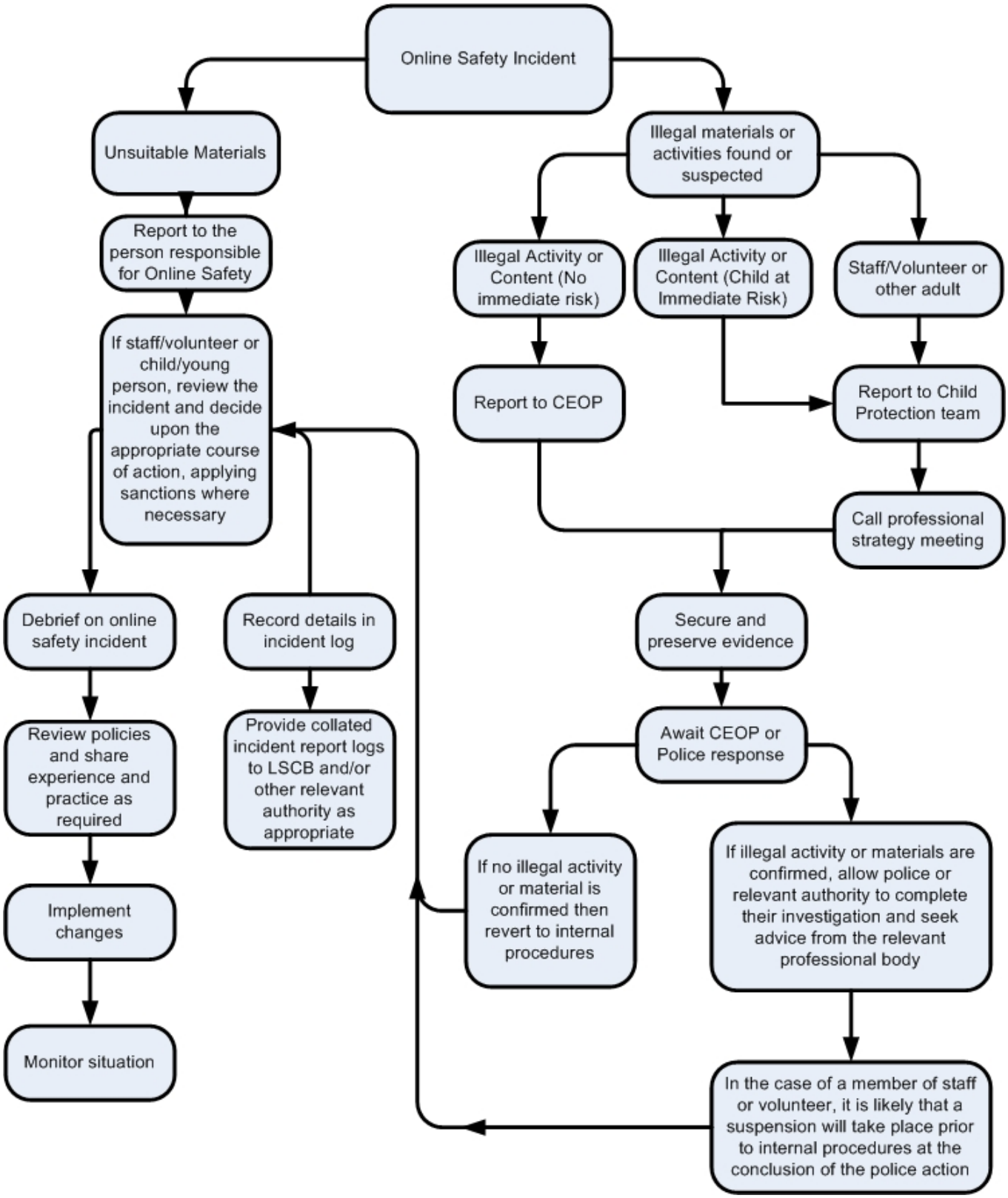
- The "administrator" passwords for the school ICT systems, one of which is used by the Network Manager and one of which is used by members of the school's Senior Leadership Team, are used for accessing confidential or sensitive information
- The school business manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Internet filtering should ensure that children are safe from inappropriate material when accessing the internet, including extremist content as defined by the PREVENT strategy
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- All teaching staff have been provided with an encrypted laptop and use the Navenby School One Drive to store documents securely in line with GDPR regulations.

Use of Images & Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained and consent forms are updated annually before photographs of students are published on the school website / social media / local media
- Parents / carers will be able to to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy, these images should not be made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the images
- Staff and volunteers are allowed to take images and videos to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images
- Images and videos should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking photos and videos that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

Illegal Incidents

If there is any suspicion that a website may contain indecent images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents.



NAVENBY CHURCH OF ENGLAND PRIMARY SCHOOL

The E-Safety Curriculum

The education of pupils in online safety is an essential part of the school's computing provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. 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 (using resources from Project Evolve & Jigsaw) as part of ICT / PSHE and is regularly revisited
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Staff should act as good role models in their use of technology 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
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study

Handling Online Abuse

Students are taught the following process for handling online abuse within or outside of school:

- do not respond to abusers
- save a copy / printscreen of any inappropriate conversations / actions
- report the user (social media / online gaming)
- block the user from contacting you
- talk to a trusted adult, who may need to involve the police

Other Useful Links

- CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website **www.ceop.gov.uk**
- IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content **www.iwf.org.uk**

Policy Approved: Full Governors meeting 20th November 2025

Signed:

Chair of Governors: …… Mr J Kirby

Head teacher ……..……Mr C Elliott