COTTESMORE SCHOOL

Anti-cyberbullying and Online Safety Policy

At Cottesmore School, we offer a modern education supported by traditional values. A growing feature of our present age is the use of various communication devices. Mobile phones are ubiquitous and offer many facilities beyond simply the ability to make a phone call. The vast majority of phones provide free messaging, have cameras and video capacity and can connect to the internet allowing access to social networking websites.

Such technology and sites can be a powerful force for good. Mobile phones and social-networking sites can help to maintain friendships and provide links between people otherwise separated by geographical distance. The internet is a vital information tool for modern life. However, there are clearly risks over content and conduct with these media. Consequently, we value pupils knowing how to use these facilities appropriately and being able to identify and respond to inappropriate use, including cyberbullying.

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".

This form of bullying is particularly insidious as it can invade home and school. Audiences can be large and reached rapidly. Words and images can easily become viral and difficult to control. The perpetrator may feel that they have anonymity and therefore feel more inclined to greater levels of bullying than might happen face to face. Images and words can be used separately or combined in an effort to belittle or ostracise others. Threats, harassment, embarrassment, humiliation, defamation or impersonation may all occur. Even where they are not the focus of an image, people may be displayed in the background of an image that is posted in a public e-space. Injury can therefore be occasioned by malice or by thoughtlessness and carelessness over the feelings of others. Such images and/or words are particularly damaging to the climate of trust within the school and may, in some circumstances, constitute illegal acts, necessitating reference to the police or other social agencies. Furthermore, offensive material may breach a provider's terms and conditions.

This policy is intended to support e-safety for parents, staff and pupils alike and to identify responses to situations where cyberbullying has occurred. Incidents of cyberbullying occurring outside school may still be investigated and dealt with by the school. As with all aspects of health and safety, e-safety is the responsibility of everybody.

Clearly, it is preferable to prevent all forms of bullying, rather than responding to it. At Cottesmore School, we have a zero tolerance approach to all forms of bullying, including cyberbullying. Pupils are encouraged to discuss potential cases with staff, and all members of the school community receive training in a range of issues to do with bullying. This is extended

to include parents and other stakeholders as appropriate. Cottesmore's network uses **Smoothwall** to restrict, manage and monitor Internet access across the school. **Smoothwall** provides real-time web filtering to help protect pupils from inappropriate or harmful online content and enables the school to manage access in accordance with its safeguarding and Acceptable Use policies.

In addition to this, the school uses a range of safeguarding and security measures, including its network **Firewall** and **Securus monitoring software**. Securus assists the Deputy Head, Designated Safeguarding Lead (DSL) and Network Manager in identifying potentially inappropriate, concerning, or harmful use of school ICT systems. Monitoring is maintained at a level proportionate to safeguarding need.

Pupils are educated in the safe and responsible use of ICT and are required to agree to the school's Acceptable Use Policy annually.

Cottesmore also has additional boundaries to ICT use that minimise the risk of cyberbullying occurring:

- pupils are not allowed to have mobile phones or other devices for social use within school. They are allowed to travel to and from school on exeats and half terms but they are instructed to hand them in to a member of staff when they arrive back in school. The items will be kept securely in a locked cupboard.
- any recordings or images made by staff may only be made with express permission from a member of the Senior Leadership Team;
- pupils and staff may not share private telephone numbers or email addresses nor actively communicate with each other on social networking sites;
- laptops and other such devices may only be used with the school's express permission;
- social networking sites may not be accessed by pupils in school time or while on the school site;
- pupils may not access on-line email accounts - like, for example, *Hotmail, Gmail* or *Yahoo* - at school. Every pupil has their own personal school email account.

Nonetheless, if cyberbullying does occur, the issue is taken very seriously. All members of the Cottesmore School community, staff, parents and pupils, are encouraged to report cyberbullying, whether they are directly involved or not, in the confidence that their concerns will be taken seriously. Any incidents of cyberbullying will be referred to a member of the Leadership Team. If the incident includes a Child Protection issue, the Designated Safeguarding Lead will be informed. A log is kept of all bullying incidents. Information will only be shared with those who need to know in order to address the situation. As with other types of bullying, re-establishing the relationship between the person bullying and the person bullied will be facilitated by the school, unless the circumstances demand permanent expulsion.

Where an allegation of cyberbullying is made, the person making the complaint will be told not to respond but to retain all the evidence, such as texts, emails, screenshots and other communication. An investigation will be commenced on the same working day. As a condition of being a pupil at the school, the Designated Safeguarding Lead, or their deputies, may require a pupil to give access to any data held on the internet, including the pupil's Facebook, or other social networking, accounts. Mobile phones, pc's and any other personal property may be searched to determine whether cyberbullying has occurred. Searching here includes, but is not limited to, a review of information held on internal and external electronic storage devices. Such measures will be used when there is a formal or informal cause for concern, including the circulation of rumours about pupil activities.

Where cyberbullying is found to have occurred, measures in the anti-bullying policy may be implemented. Click on this link to find the Anti-bullying Policy.

Additionally, victims of cyberbullying will be encouraged to reconsider what information they keep and make publicly available on line, in order to prevent future occurrences. The offender will be required to stop immediately any inappropriate activities and remove unacceptable postings, whether textual, visual or auditory. Providers may be contacted to facilitate the removal of unacceptable material. Whether material is unacceptable will be decided by the school. Sanctions against the offending pupil, identified under the general anti-bullying policy, may be imposed subsequently.

Further measures in the case of cyberbullying may include:

- the pupil having access to ICT limited or withdrawn entirely in school;
- the incident being reported to the relevant service provider, potentially causing services and facilities to be withdrawn;
- notifying the police;
- where the school is unable to confirm the identity of a cyberbully or is caused to believe that there may have been an incident of 'identity theft', the police may be informed.
- In all cases, parents/carers of both the person bullying and the recipient will be informed.

With the increasing use of Artificial Intelligence (AI), **Smoothwall** also provides controls specifically designed to manage access to generative AI services and other AI-based tools.

The **"Unsafe AI Chat"** category enables AI services identified as presenting a potential safeguarding risk to be blocked.

The **"AI Tools"** category allows the school to manage access to AI services in accordance with school policy, including blocking AI tools that have not been approved for pupil use.

This policy will be reviewed annually and in line with legal developments. It is to be read in conjunction with the school anti-bullying policy and with an understanding of the school's Acceptable Use Policy for ICT, which every user agrees to, and other relevant documents.

Reviewed by Deputy Head September 2026
To be reviewed September 2027

There are many agencies that help to address issues of ICT misuse:

CEOP http://www.ceop.gov.uk Child Exploitation and Online Protection Centre (CEOP) is part of UK policing and tracks and brings offenders to account either directly or in partnership with local and international forces.

Think U Know http://www.thinkuknow.co.uk Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UKCCIS Link1 Link2 The UK Council for Child Internet Safety (UKCCIS) 'Click Clever Click Safe' Campaign strategy aims to create a safer online environment, gives everybody the skills, knowledge and understanding to help children and young people to stay safe online and inspire safe and responsible use and behaviour.

Childalert http://www.childalert.co.uk/ This campaign encourages children to keep safe online by keeping personal information private, blocking messages and reporting inappropriate online behaviour. This new digital code is intended for use by schools, retailers and social network sites and aims to be the 'green cross' code for internet safety.

Childnet http://www.childnet-int.org Childnet is a non-profit organisation working with others to "help make the Internet a great and safe place for children". The website gives news and background to Childnet's work and serves as a portal to Childnet's award-winning projects

IWF http://www.iwf.org.uk Internet Watch Foundation (IWF) hosts the UK Hotline for reporting illegal online content specifically relating to child sexual abuse, criminally obscene as well as incitement to racial hatred

Digizen http://www.digizen.org Digizen provides information about using social network sites and social media sites creatively and safely. It provides tips for evaluating these online resources and examples of how to use them to support informal and formal learning.

Kidsmart www.kidsmart.org.uk A fun educational anti-cyberbullying resource created by Childnet

Safe www.digitalme.co.uk/safe Safe is a programme of practical activities that develop young people's skills, self-confidence and safety awareness when using social networking sites.