St Olave's Grammar School

CYBERBULLYING/INTERNET MISUSE POLICY

1. Definition and Scope

Cyberbullying involves the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. It differs from other forms of bullying in that it can invade the home and personal space, be anonymous, attract the attention of a wide audience, and be characterised by the difficulty of controlling electronically circulated messages. It can, and does, affect both students and staff. (One –off incidents may be very serious and will always be dealt with but may not fall within the definition of "bullying". They are classified as misuse rather than bullying)

Cyberbullying will often originate off site and is becoming an increasingly serious problem with the growth of social networking sites. The School is empowered by law "to such extent as is reasonable" to regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff.

2. Forms of Cyberbullying/Internet Misuse

Typical examples of include:

- **Threats and intimidation** using mobile phone, texts, email, comments on websites or social networking sites or message boards
- **Harassment or stalking** repeated, prolonged, unwanted texting whether offensive or not is a form of harassment. Monitoring a person's online activities, sometimes referred to as cyber-stalking. Using public forms, such as message boards, chatrooms or social networking sites to repeatedly harass, or to post derogatory or defamatory statements in order to provoke a response from the target.
- **Vilification/defamation** through posting upsetting or defamatory remarks about an individual online, or name-calling using a mobile device.
- **Ostracising/peer rejection/exclusion/inciting hatred,** using social networking sites to exclude someone.
- **Identity theft, unauthorised access and impersonation,** through accessing someone else's account by finding out or guessing their username and password information. Hacking somebody's account in this way is illegal under the Computer Misuse Act 1990. Unauthorised access to somebody else's account can lead to:

- Posting private information on public sites, or via email in order to harass or humiliate.
- Deleting information
- Impersonation. There have been cases where a bully has sent out nasty messages to everyone on a pupil's buddy list, and images and contact details have been posted to public sites with invitations to contact them.

- **Sending/forwarding Images.** Once pictures are made public it becomes very difficult to contain them. They can be circulated via phones, email and postings to social networking sites. Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal under the Protection of Children Act, 1978. Such pictures are illegal even if they were taken for 'fun' or by 'willing' parties. Images cannot be taken without the permission of parents/carers.
- **Sexting**, sending messages with an inappropriate sexual content
- **Manipulation,** for example putting pressure on someone to reveal personal information.
- **Social Networking Sites**

  Users of these sites may post a lot of detailed and personal information about themselves and their friends. It can then be misused. Such sites can be abused in several ways:

  - Nasty comments may be posted.
  - People might use their own sites to spread rumours or make unpleasant comments, or post humiliating images or videos
  - Fake profiles are also fairly common in order to pretend to be someone else.

3. St Olave's Behaviour Policy on Cyberbullying

There are no excuses for cyberbullying; students need to be aware that their actions have severe and distressing consequences and that participating in such activity directly or indirectly will not be tolerated. Students should understand that:

- The school has a 'zero-tolerance' attitude towards proven cases of cyberbullying
- Any reported incidents of cyber-bullying will be investigated whether they involve the school network or not.
- The school network will be monitored daily and examples of inappropriate emails received or sent, and inappropriate website content will be captured with user details, date and time, and machine IP address and such material will be used as evidence.
- Possible witnesses will be interviewed
- Internet service providers, mobile phone companies and social networking sites will be contacted to obtain relevant user information as appropriate

- Police involvement will be sought if considered appropriate
- Once the person responsible for the cyberbullying has been identified appropriate sanctions will be applied consistent with the School's Anti-Bullying Policy and Network Agreement. These could include disabling school network access (either on a temporary or permanent basis) removing the right to use a mobile phone on the school site, internal and external fixed term or permanent exclusion.
- The defence that someone else used my account will not be acceptable (see 4 vi)

4. St Olave's Education Policy on Cyberbullying

The School will:

- Promote understanding and awareness of cyberbullying through presentations/discussion at year assemblies, and in the PSHE programme, and ensure students are aware of the school's duty of care for activities affecting the school community both within and outside school.
- Post and/or publish on the School's website information about cyberbullying and school policy.
- Ensure reporting of cyberbullying is straight-forward, confidential and followed through
- Ensure students understand that any reported incidents will be reported directly to the relevant internet service provider or mobile phone company
- Review student ICT acceptable use policy and ensure clarity in respect of rules relating to cyberbullying, sanctions for misuse and issues relating to confiscation.
- Ensure students understand the importance of keeping account information private and secure. Students have a duty to keep their password secret and not to knowingly allow another user to use their account.
- Promote the use of 'filtering software' within school and maintain a log of relevant incidences, use recorded incidents to identify sites that should be banned, and to remove inappropriate material. Ensure that students are aware that such monitoring software is in use.