Cyberbullying

St Dunstan's College

BACKGROUND

St Dunstan's College has a duty to protect pupils and staff from online activities that are harmful and damaging and which can, in some circumstances, constitute a criminal act. Cyberbullying poses a growing challenge and the College possesses a clear framework of policies giving guidance in this area. The School ensures too that pupils and staff are apprised of the College's expectations. This policy outlines in greater detail how pupils, parents and staff can work together to foster an environment in which Cyberbullying is not tolerated and where there is effective detection of and sanction for those involved in it.

This policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection
- Anti-bullying Policy
- Expected Pupil Behaviour and College Rules
- ICT Policy and Pupil Acceptable Use Agreement

DEFINITION OF CYBERBULLYING

Cyberbullying is bullying that takes place using electronic technology. This includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

Examples of cyberbullying may include:

- Creating or interacting with mean text messages, emails, instant messages or posts on social networking sites
- Rumours sent by text or email or posted on social networking sites
- Spreading or interacting with embarrassing pictures, videos or websites
- Sharing nudes or semi-nudes without consent (this behaviour is also illegal if the person in the image is under 18)
- Threatening text messages, phone calls emails or posts on social media sites
- Creating fake profiles on social media sites
- Gaining unauthorised access to someone's gaming, email or social networking profile.
- Creating media that have stories, pictures, or jokes ridiculing others.

Cyberbullying is different from 'in-person' bullying because:

- Cyberbullying can happen 24 hours a day, 7 days a week, and reach a child even when he or she is alone.
- Cyberbullying messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source.
- Deleting inappropriate or harassing messages, texts and pictures is extremely difficult after they have been posted or sent.
- Children who are being cyberbullied are often bullied in person as well. Additionally, children who are cyberbullied have a harder time getting away from the behaviour.

POLICY

1. St Dunstan's College recognises the particularly detrimental effects of cyberbullying on children and will deal with all allegations of cyberbullying quickly and seriously in accordance with the College's Anti-bullying policy.
2. All staff receive training in e-Safety in order to model best-practice and to support pupil e-Safety education.
3. E-Safety is taught to all pupils through Stuart and Computing lessons, special assemblies, external speakers and throughout the entire curriculum.
4. Support is provided to parents on how to help their children engage safely and responsibly with social media, through information evenings, advice in the school newsletter and signposting to other sources of support and advice.
5. The College recognises the possible criminal nature of cyberbullying, and the DSL and other Pastoral Leaders within the school attend regular training to keep up-to-date on legal responsibilities.

PROCEDURES

What to look for:

Pupils who are being cyberbullied may find it difficult to talk about their experiences. Research suggests that many children who are being cyberbullied don't tell their parents or teachers, so it's important to recognise the signs. They can be hard to spot, but some things to look out for are:

- Sudden or unexpected cessation in using their computer, mobile phone or tablet
- Appearing nervous or jumpy when an instant message, text message or email appears
- Avoiding school or socialising in general
- Being angry, depressed or frustrated after using their phone, computer or tablet
- Becoming withdrawn from friends and family members

What to do:

If you are the victim:

- Don't retaliate or reply to nasty messages.
- Save the evidence – text messages, online conversations, social media posts, etc. Sometimes, taking a 'screenshot' is the easiest way of preserving evidence of cyberbullying.
- Use 'block sender' features on your phone or social media sites to prevent further bullying.

- Tell someone about the incident: ideally, you should tell your Form Teacher, Tutor or Head of Year, but any staff member (including the Counsellors and the Chaplain), friend, parent, or trusted adult should be able to help you or find someone who can.
- If you don't want to talk to a member of staff about the incident, ask a friend, family member or trusted adult to talk to a member of staff on your behalf.

If a pupil witnesses cyberbullying:

- Do not be enticed into sending retaliatory messages or posts.
- Do not do nothing – if you see any messages or posts which are hurtful or intending to cause harm, you MUST report this to the College. You can be sanctioned as complicit in a cyberbullying offence later on if it is discovered that you were a 'passive bystander' (e.g. party to an online conversation, even you weren't contributing to it) and did not report the bullying. **You are a bystander if you read it, see it, or hear about it.**
- Accompany the victim to a trusted adult, or suggest that you see their Tutor or Head of Year on their behalf.
- If possible, save the evidence of the bullying via screenshots for example.
- Remember to report the post if it's on a social networking website. Anyone who has an account on Facebook or Instagram has the ability to report offensive and unacceptable content (see below for more tips on how to protect and report offensive posts on Social Media Platforms).

If a member of staff witnesses an incident of cyberbullying or has it reported to them:

- Reassure and support the pupils involved.
- If the pupil has evidence of the cyberbullying, with the pupil's permission take their phone or device on which the evidence is stored directly to the DSL for further advice.
- Advise them that you are required to pass the details on to the relevant member of the pastoral team (DSL).
- Report the incident on MyConcern, or if MyConcern is not available report the incident directly to the DSL.

What will happen?

- Cyberbullying incidents will be dealt with as outlined in the College Anti-bullying policy.
- There is an increased likelihood of a cyberbullying incident to involve criminal offence than in-person bullying.
    - Any incident involving images or videos generated by or of children under the age of 18 that are of a sexual nature will be dealt with according to the College policy *Sending Nudes and Semi Nudes* and the law.
    - Under the Malicious Communications Act 1988, it is an offence for a person to send an electronic communication to another person with the intent to cause distress or anxiety or to send an electronic communication which conveys a message which is indecent or grossly offensive, a threat, or information which is false and known or believed to be false by the sender. In addition to College-level sanctions, incidents of this nature will be reported to the Police.

- Under the Protection from Harassment Act 1997, it is an offence to send a 'credible threat' of violence, harassing communications targeting specific individuals or 'cyberstalking' communications targeting specific individuals. In addition to College-level sanctions, incidents of this nature will be reported to the Police.
- Under the Crime and Disorder Act 1998, it is an offence to send any race- or religion-based threats or aggravated communications targeting specific individuals. In addition to College-level sanctions, incidents of this nature will be reported to the Police.
- Under the Criminal Justice Act 2003, it is an offence to send any disability- or sexual orientation or transgender identity-based threats or aggravated communications targeting specific individuals. In addition to College-level sanctions, incidents of this nature will be reported to the Police.

How can I keep my content secure?

- It is good practice to ensure your privacy and security settings allow you to control who can see the content you share. Please be aware however, that content can still be easily screenshotted and shared more publicly.
- Ensure your devices are protected with a pin or passcode to protect your personal data, images, videos and accounts.
- Make sure you have strong passwords on all your accounts and you update these passwords on a regular basis. Remember not to share your password with anyone.
- Remember to log out of accounts when using public WiFi connections.
- Discuss these same issues with your friends and family as you could become a target if their privacy settings are not up to date.
- Always be sure who you're befriending or talking to online. Never give out your personal details, including your mobile number and social networking sites if you don't know the person you're talking to.
- Use your school email address for school business and personal email for your private life; do not mix the two accounts. This includes file sharing websites e.g. YouTube.

SOCIAL MEDIA PRIVACY SETTINGS

Instagram

- If you see evidence of unacceptable or offensive material on INSTAGRAM, remember to take a screenshot and show this evidence to a parent/guardian/staff member.
- **Blocking** – When you use the blocking feature, the person you block will not longer view your posts or be able to search for your Instagram account.
- **Report It** – You can report inappropriate posts, comments or people by using the built-in reporting features in the app.
- **Delete or Reporting comments** - You can flag or delete a comment as abuse or spam by swiping left on it.
- **Privacy Settings** - You can adjust your privacy settings to make your account private. This means that anyone who wants to see your photos or videos, followers, or following lists will have to send you a follow request for you to approve or ignore.
- **Location Settings** - Users choose when they share location on each post.

WhatsApp

- If you see evidence of unacceptable or offensive material on WhatsApp, remember to take a screenshot and show this evidence to a parent/guardian/staff member.
- **Blocking** - If you block someone, they can no longer send you a message, however you will need to delete someone as a contact in your phone book if you don't want them to see your profile on WhatsApp.
- **Report It –** It's important to screenshot the offending text/picture/video and to provide as much information as possible to WhatsApp as they won't be able to see the message otherwise.
- **SPAM** - If you receive a message from an unknown number, you will immediately be asked if you know this contact or if you would like to report it as spam. You should **never** accept or respond to find out who the message is from.
- **Privacy Settings** - To control who can find your profile picture and your status, or when you were last online, there are privacy settings that can be adjusted so either 'everyone' on WhatsApp can see your profile picture, just 'your contacts' which are the contacts in your phone book, or nobody.

TikTok

- **Privacy settings** - If you have a private account, your friends will need to follow you and you will need to approve them in order for them to see your videos. Please check your privacy settings on TikTok.
- **Blocking** - If someone is bothering you on TikTok, you can block them.
    - Find the user's profile. The user can be found in your following/fans list.
    - Tap on the triple dots at the top right corner. This will open a menu of options.
    - Choose "Block" and confirm.
- **Deleting** - If a fan is bothering you, you can swipe left to delete them.
- **Reporting** - If you see inappropriate content on TikTok, you should report it by clicking on the button with three dots and then click 'report abuse'. Should you violate the community guidelines, your account may be removed without warning.

Facebook

- To block messages from someone on Facebook:
    - Click at the top right of the page
    - Open the conversation with the person you'd like to block
    - Click in the top right of the chat box
    - Click Block > Block Messages and Calls
- To change who can add you as a friend:
    - Click the top right of any Facebook page and click Settings.
    - Click Privacy in the left column.
    - Click Edit next to **Who can send you friend requests**?
    - From the dropdown menu, click **Everyone** or **Friends of Friends**.
- If someone's bothering you on Facebook, the best way to stop them is to block them. You can also Unfriend them so only your friends can post on your timeline.

Snapchat

- **Blocking** - When you use the blocking feature, the person you block can't view your snaps or your Snap story and they can't send you snaps either.
- **Privacy settings** - Only those who you add as friends can view your snaps. If someone who you haven't added sends you a snap, you will get a notification, but you have to add them as a friend to see what they sent you. You can change who can see your snaps by changing your privacy settings.
    - On Your Camera Screen, tap on the Bitmoji (the ghost icon in the top left) to go to your Profile Screen.
    - On your Profile Screen, tap on the "Settings" gear icon in the top right.
    - Scroll down until you come across the "Who Can …" section.
    - Select an option, and tap on the back button to confirm.
- **Dealing with the Find Friend feature**
    - This feature lets people who have access to your phone number find your Snapchat profile by using your number.
    - Tap on the "Settings" gear icon in the top right of your Profile Screen.
    - Tap on "Mobile Number."
    - Look for "Let others find me using my mobile number."
    - Tap the icon next to it to exclude your number from this feature.
- **Reporting** - If you experience harassment, or bullying, you can report inappropriate snaps.
    - Press and hold on the Snapchatter's name, tap 'More,' and tap 'Report.'
- **Location** - Locations in Snapchat are shown in 'Snap Maps', there are three options for who can see your location; only me, select friends and my friends.

To fully secure your social media accounts, you should consider turning on two-factor authentication.