Date: Nov 2026
Next review due: Nov 2027
Responsibility: Digital Strategy Leads

DAME ALLAN'S SCHOOLS

PUPIL AND PARENT SOCIAL MEDIA AND AI GUIDANCE

Online social media platforms, such as Instagram, Snapchat, TikTok, YouTube and X, and messaging apps such as WhatsApp, are now pervasive in society, including in the lives of many of our pupils. These networks are designed to be extremely attractive to children and young people in order to gain as much of their attention as possible. However, they open up a whole range of social and pastoral issues which schools have to deal with on a frequent basis. Generative artificial intelligence (AI) tools are now just as widely used by young people and bring new risks of their own. In order to do the best we can to keep children safe online, parents and children need to be aware of the following:

1. Whatever is written online remains traceable permanently, and is potentially visible to everyone. This includes messages and images that are designed to disappear, which can easily be screenshotted or recorded. Posting certain comments or images on sites such as those mentioned above can quite easily lead to someone committing a criminal offence and the evidence trail is extremely easy to follow.

2. Ultimately, schools have no power to control what a pupil puts on their own computer/mobile device outside school hours. However, the Schools will investigate the misuse of social media, messaging apps or AI tools where it results in bullying, abusive behaviour or harm involving their pupils, and have safeguarding duties to act on any concerns that come to light; this includes the use of such technology outside school hours.

3. Sharing nude or semi-nude images, videos or live streams of young people under 18 (previously known as "sexting") is one of the most common safeguarding concerns schools deal with. Pupils and parents need to be aware that it is illegal to create store, possess, send, ask for, receive or distribute an indecent image of a young person under 18 years, including images children have taken of themselves. This includes images created or altered using AI, such as "deepfakes" or images created with "nudify" apps. The Schools will take appropriate action to safeguard, support and educate pupils involved in such incidents and will impose

sanctions against pupils involved in aggravated cases (the deliberate distribution of images to bully, demean, threaten or harass), which may result in suspension or exclusion. In some circumstances the Schools must report cases to the police and Children's Social Care. The Schools' full procedures are set out in the Safeguarding and Child Protection Policy.

4. If a pupil or parent becomes aware that a nude or semi-nude image has been shared, they should not view, copy, forward or share it, and should tell the Schools' Designated Safeguarding Lead (DSL) as soon as possible. The DSL will advise on deleting it. Young people under 18 can ask for nude images of themselves to be removed from the internet using Report Remove, run by Childline and the Internet Watch Foundation.

5. Financially motivated sexual extortion ("sextortion") is a fast-growing risk, particularly for teenage boys. Criminals, often posing as young people, persuade a child to share an image and then threaten to send it to family and friends unless they pay. Children should know that they will not be in trouble for asking for help. They should stop all contact, not pay, keep evidence such as usernames and messages (but not the image itself), and tell a trusted adult straight away. Concerns can be reported to the police through CEOP (www.ceop.police.uk).

6. Most social media sites currently require the user to be at least 13 years of age. Users who are under 13 years of age break the terms of the site's use. If children give a false age in order to open an account they will be exposed to material deemed to be suitable for that false age. So if a child of 8 claims to be 13, parents need to be aware that once that child actually reaches 13 years of age, they will have access to all 18+ adult material.

7. The Government has announced that, from spring 2027, social media platforms will not be allowed to provide accounts to children under 16, and will have to check users' ages. Messaging services such as WhatsApp are not included.

8. Pupils are potentially exposed to malign influences which they would not normally encounter other than via these networks. This may include content/individuals linked to radicalisation, extremism, misogyny and misinformation.

9. If pupils do use social media, we suggest the following specific guidance be followed:

    a. Different social media sites have different age limits for users, and these will change in 2027 . Parents should make themselves aware of the limits on sites their children are using. The NSPCC site: (https://www.nspcc.org.uk/keeping-children-safe/online-safety/social-media/) has information on the majority of social networking sites and we recommend you visit this site to familiarise yourselves with the sites or apps that your children are using.

    b. Pupils must regularly ensure their privacy settings are at the maximum.

    c. Pupils must never disclose their full name, age, date of birth, phone number, e-mail address, address, school or any other personal data. They should be aware that they can be identified by those not known to them if they upload photos of themselves or others and they do not have their privacy settings correctly set.

d. Location sharing, such as Snap Map on Snapchat, and on other apps where such a feature exists, should be disabled as viewers of posts may be able to locate your child.

e. Pupils setting up groups or group chats must ensure that the content of those pages is not abusive, bullying or offensive to any general reader, even if it is deemed acceptable to the members of the group.

f. Content, which refers to the Schools, can have a very damaging effect on the Schools' reputation even if it may appear to be "just banter" or "harmless fun" to the participants. Dame Allan's Schools will always take rigorous action to protect our reputation if such material comes to light, including the possible imposition of disciplinary sanctions on any pupil found to be creating, adding to or viewing such sites.

g. Pupils must never create, share or ask for AI-generated or edited images, video or audio of another person, including pupils or staff, without their permission. Fake images of a sexual nature will be treated in the same way as real ones

h. Parents are encouraged to talk to their children about how they use social media and AI tools, to check regularly the type of content their children are exposed to online and to support the Schools in their efforts to keep pupils safe online.

i. Pupils should assume that anything they post or share online could become public and remain accessible indefinitely

10. Parental attention is drawn to the issues mentioned here at the New Parent Information evenings.

11. Generative Artificial Intelligence (AI) such as ChatGPT, Gemini and Copilot, and AI features built into other apps, such as My AI on Snapchat, are increasingly widely used in society. Under the explicit instruction of a teacher, pupils can use AI tools to generate data and content or to enhance learning. This use should be using the Securly Chat feature. In no circumstances should AI be used for cheating or plagiarism. More guidance can be found in the Whole School AI Policy.

12. This guidance should be read in conjunction with the Whole School Policy on the Acceptable Use of Electronic Devices and Information Technology Systems, the Safeguarding and Child Protection Policy and the Whole School AI Policy.