EST. 1914

THE CARDINAL VAUGHAN MEMORIAL SCHOOL

Amare et Servire

THE CARDINAL VAUGHAN MEMORIAL SCHOOL TRUST

ONLINE SAFETY POLICY

This policy and procedure was approved and adopted by The Cardinal Vaughan Memorial School on 1 February 2021 and is reviewed annually.

THE CARDINAL VAUGHAN MEMORIAL SCHOOL

ONLINE SAFETY POLICY

INTRODUCTION

Although the potential of electronic media to enhance educational opportunities is broad and powerful, and to that extent to be welcomed, the growth in its use does expose staff and pupils to a greater degree of risk, which must be carefully managed.

RATIONALE

Online Safety depends on addressing three broad areas of risk:

- content: being exposed to illegal, inappropriate or harmful content; for example: pornography, fake news, racist, misogynistic, self-harm, suicide, anti-semitic, radical and extremist;
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults for the purposes of grooming children; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, sharing others explicit images and online bullying.

The School's approach therefore involves effective practice at a number of levels:

- responsible ICT use by all staff and pupils;
- sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use; and
- safe and secure Internet access including monitoring and the effective management of filtering.

PROMOTION OF ONLINE SAFETY

The School explicitly addresses the issue of Online Safety for pupils in the curriculum and in PSHE in order to encourage responsible and self-regulating use of the internet and electronic media. Parents are also provided with a booklet on how to keep their children safe. In addition, in order to promote a safe learning environment, websites accessed by pupils and staff are both filtered appropriately and actively monitored. Parents on behalf of their son are required to sign an acceptable use policy before starting at the school in first year.

MANAGEMENT OF INTERNET USE AND ELECTRONIC DEVICES

The following applies to any use of the Internet in which the School is concerned, whether such use is made at the School or elsewhere.

- In using the Internet, pupils and staff must adhere to the Catholic ethos of the School.
- No computer facilities (including Internet access) will be used inappropriately or in any way that might be considered to be detrimental to fellow pupils, staff or the School as a whole.
- Pupils must not attempt to visit any site that could be considered offensive to their parents, teachers or peers. This includes pupils in the Fifth and Sixth Forms using smart phones and their personal data (4G or 5G).
- Pupils must not give out any personal information over the Internet (full names, addresses, telephone numbers, photographs, videos and so on). This includes publishing such information on web pages, in particular on social networking sites. To protect our pupils' and staff's privacy, anyone wishing to publish material pertaining to the School must first seek permission to do so from the Head of School.
- Pupils must not send any email or text, or create any social networking posts that contain material which could cause offence, or which conceals their identity from other pupils or members of staff.
- The Head of School will normally exclude a pupil from the School, on either a fixed–term or permanent basis, for involvement in the production or maintenance of Internet websites, either on or off the School's premises, the contents of which might damage the good name of the School, or any individuals within it.
- If a pupil receives any offensive material by email, text or social networking posts he or she must report the matter to a member of staff immediately.
- If a member of staff receives any offensive material by email, text or social networking posts he or she must report the matter to the Head of School
- Staff and pupils should only use the School's e-mail account to communicate with each other electronically.
- Pupils and staff must not attempt to download software from the Internet on to the School's Computer Network. They must at all times, make appropriate use of the system.
- Pupils who fail to observe these rules will be referred, in the first instance to the Head of Year. Serious or persistent offenders may expect to receive serious sanctions.
- All pupils are to comply with the terms of the Computer Misuse Act at all times. Any pupil responsible for any breach of the act may expect to receive the most serious of sanctions.
- No pupil may copy or attempt to copy another pupil's or teacher's files or records.
- No pupil may use hacking or spy software, in any form, on the School's network.
- Wearable technology such as Smart watches is not permissible at School. These must be turned off and kept in lockers while on School grounds.
- Smartphones are banned for pupils in the First to Fourth Forms.
- Smartphones are allowed for pupils in the Fifth and Sixth Forms, but their use is strictly restricted to break times and Private Study.

- The showing or circulation by any pupil of inappropriate material of any description to others through the use of a mobile telephone, tablet computer or any such similar device may result in a suspension or permanent exclusion from the School.
- The use of any device for the recording of audio, still or moving images at the School or of the staff is not permissible without the prior consent of the Head of School.
- The use of video sharing websites (e.g YouTube) at School is strictly for academic purposes.