Jeannine Manuel School
International understanding through a bilingual education

IT CODE OF CONDUCT FOR PUPILS

1 INTRODUCTION

Jeannine Manuel School ("the School") expects all users to respect the systems provided and to use them responsibly, securely and legally. By logging onto the School's IT networks, all pupils are deemed to have read this IT Code of Conduct and agreed to adhere to its terms and conditions, as well as those set out in the School's E-Safety Policy.

The School makes its ICT systems and networks available to support the educational and professional activities of pupils, staff and visitors on the understanding that they will be used appropriately at all times. Any activity that threatens the integrity or security of systems or that corrupts or compromises information, that threatens the reputation of an individual or the School or contravenes the law will be subject to disciplinary action. The School also prohibits access to any illegal, harmful, or inappropriate content.

Acceptable use includes, but is not restricted to, the points detailed below. The code is updated routinely and the latest version is available on the School's website.

2 NETWORKS AND DATA SECURITY

2.1 The security of the School's ICT systems, whether owned by the School or other organisations or individuals, must not be compromised. Pupils may not disconnect any item of computer equipment from the School's IT networks, nor are they authorised to install any equipment onto the School network or software on school-owned equipment.

2.2 Pupil mobile phones and any other devices which have the capacity to send and receive messages, including smart watches, must be switched off and placed in the student's bags at all times when within the school premises. Students in Middle School should use the dedicated "phone pouch" system as instructed. Mobile phones found to be switched on during the school day will be confiscated and returned at the end of the day. Repeat issues of this nature may face more severe sanctions at the discretion of the relevant section Head.

2.2.1 The only exception concerns personal laptops which are authorised in Y12 and Y13 at the discretion of the teacher.

2.3 This code covers all access to or through school systems by pupils using their own portable or handheld devices (e.g. laptops connected to the wireless network, smartphones synchronised with school email accounts).

2.4 Access to the network may only be made using the authorised account and password issued to that user, which must not be shared with other people. To protect themselves, users should never leave a network account logged on at an unattended machine, and users must always log off when finished, whether accessing systems in School or remotely.

2.5 We encourage students to use strong and secure passwords for their accounts.

2.6 Use of school systems for personal financial gain, gambling and political purposes or advertising is forbidden.

2.7 Malware (viruses and spyware) must not be introduced to school systems, maliciously or inadvertently.

2.8 Pupils may not use front-of-class equipment provided for teaching staff in classrooms unless under the supervision of teaching staff.

2.9 All network users must terminate remote access securely by logging off and shutting down at the end of all sessions; portable devices and smartphones synchronised to school systems must be protected by automatic locking and passcode access.

3 The Law

All users are subject to legal frameworks including the Data Protection Act (2018) and Data and Computer Misuse Acts (1990). Copyright and intellectual property rights must be respected.

4 Personal Use

4.1 Users of the school systems may not store large volumes of personal emails and data (e.g., multimedia music or image files) on the school's networks.

4.2 In addition, students should not use the school's IT systems for anything other than educational purposes, unless approved by staff.

5 Communication

5.1 Users are responsible for the e-mails they send and for contacts they make; email should be written carefully and politely. As messages may be forwarded, email is best regarded as public property. Anonymous messages, emails sent from another user's account, chain messages and all-pupil emails must not be sent.

5.2 School systems must be used for all online communications between staff and pupils. For the protection of staff, pupils and the School, social networking sites and other public forums should not be used for communication between staff and pupils. Pupils become leavers from September following their final term at school.

5.3 All users are expected to check email accounts daily during term time.

5.4 Users are responsible for deleting old and non-essential email messages (both sent and received) every term and must ensure that their account file space limits are maintained and work backed up. Users will be expected to reduce storage volumes on their email accounts if they exceed acceptable quotas, as determined by the IT Department.

6 Online Activity

6.1 The School reserves the right to block and/or restrict access to certain websites on the grounds of inappropriate content, excessive bandwidth or timing. Requests to unblock restricted sites can be addressed to the IT Department.

6.2 Covert filming, photography or audio recording of any member of the school community is forbidden. The distribution or dissemination of materials by any means captured in this way is a serious breach of this Code of Conduct and will be viewed as cyber-bullying if it causes humiliation or offence.

6.3 Information about the School should not be recorded on pupils' social networking pages or other public forums. You are advised not to disclose personal details (yours or those of others) such as names, address, contact details or any other identifying information, on these sites to protect yourself from fraud, theft, abuse or access by external organisations that may base personal references on the information you post. If you have inadvertently accessed inappropriate material, would like to report abuse, are concerned about something you have seen online, or would like to report a suspected breach of this Code of Conduct, please speak to your Form Tutor, Division Head or to the Head. The School may exercise its right by electronic or other means to

monitor the use of the school's computer systems by checking websites accessed, intercepting e-mails and deleting inappropriate material if it believes unacceptable or unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorized, unlawful or inappropriate. For more information about how your data is processed for the purposes of security and safeguarding, please see the Privacy Notice on the school website.

6.4 Cyber-bullying, like all types of bullying, will not be tolerated by the School. In accordance with our Anti-Bullying Policy, disciplinary action will be taken against pupils found to have committed acts of cyber-bullying.

6.5 Similarly, any incidents involving digital child-on-child abuse will be dealt with in accordance with our Safeguarding Policies.

6.6 The School has developed a robust E-Safety Policy to ensure that pupils are taught how to safely access and use the internet. While the internet provides wonderful learning opportunities, you should also be mindful of the inherent risks that come with using online technologies.