The Sandon School

Information, Communication, Technology (ICT) and E Safety Policy

Last Adoption Date: July 2018

Next Review Date: Summer 2021

Introduction to information and communication

1. The Sandon School is committed to ensuring the safe, responsible and professional processing of information and its communication with or without technology and ICT use. This policy supports the culture of the School of openness as regards all forms of communication in particular paper, electronic and verbal.

2. The School will comply with all legal requirements relating to information and communication. It will obtain appropriate licences and have adequate security arrangements in place. The School will comply with legislation relating to information and communication in particular Data Protection Legislation (DPL), Freedom of Information (FOI) and Intellectual Property rights such as Copyright.

3. The processing, storage and retention of personal information/data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed.

4. The school community will ensure that no communication is made that may be considered inappropriate or a misuse of information/ data or will bring the School into disrepute.

5. The school community must treat all methods of communication with respect. Any facility may be changed or withdrawn at the discretion of the School. If appropriate, it may be subject to a charge.

6. This policy links with other school policies such as Code of Conduct, Data Protection and Freedom of Information, Safeguarding, Discipline, Behaviour, and Equality.

7. Breaches of this policy will be a disciplinary matter; a serious breach by a student could result in exclusion. A serious breach by a member of staff could be gross misconduct and lead to dismissal. In certain circumstances, a breach of this policy could result in the matter being reported to the police or other appropriate authorities.

8. There will be no electronic recording made of any verbal communication unless required by the policies or procedures of the School without the consent of all appropriate parties. If there is any disagreement as to whether a recording should be made this will be determined by the Headteacher or if appropriate the Governors managing the issue.

9. There may be a small amount of personal use of the School's equipment. Where this occurs this policy and other School policies will apply.

Responsibilities

10. The Governing Board will ensure that the School complies with all appropriate legislation and that this policy and all related procedures, statements and rules are implemented and monitored.

11. The Headteacher will implement this policy and any related procedures, statements and rules ensuring that all members of the school community are aware of their responsibilities. The Headteacher will report periodically to the Governing Board on the operation and effectiveness of this policy.

12. All staff with management roles have an additional responsibility of ensuring that all members of their team are aware of and understand this policy.

13. All staff and students must comply with this policy and be educated in safety and undertake appropriate training.

14. All members of the school community including parents, visitors and contractors should where appropriate be made aware of this policy.

15. All staff and students have a responsibility for the security and responsible use of the equipment provided for their use. If permission is given for any such equipment to be removed from the school premises, care must be taken over the security of and access to personal data that maybe contained on it.

16. When accessing any personal data away from school, particular care must be exercised to ensure that no information is stored on any non school equipment, access is restricted to yourself and your pin code or password is not shared with any other user or saved to your browser.

17. Guidance on the acceptable use of ICT for students is set out below and guidance for staff is within the School's staff Code of Conduct policy.

18. No school equipment may be taken abroad without approval of the Business Manager

Teaching and Learning

19. All ICT and communication facilities should be valuable tools for education encouraging development and understanding, but care must be taken at all times with the communication of personal opinions.

20. When the students are using school ICT and communication facilities, staff will be responsible for guiding students to appropriate materials. They will encourage parents to provide guidance and support where appropriate.

21. All staff and students have a responsibility to use ICT and communication facilities legally, responsibly and with due care.

22. Particular care must be exercised in the communication of any personal data in order to comply with DPL. Personal data must not be communicated to third parties unless agreement has been provided. If in any doubt, please check with the Business Manager.

23. The school has responsibilities with regard to sustainability in particular replacing the use of paper whenever possible. Electronic and/or paper communication should never replace personal contact when this is appropriate.

Security

24. The School will adopt sound professional practices, procedures and schedules of training to protect secure information and to reduce the risk of inappropriate communication of secure or confidential information. This may include the inspection, monitoring, review and interception of communications as authorised by the Headteacher. This will be reasonable and proportionate but may involve outside agencies.

25. The School will make all reasonable provisions to ensure that adequate security systems are installed to protect the accidental access of inappropriate information. The School will take all reasonable measures to protect all members of its community from spam, grooming, viruses and cyber-bullying and all other forms of inappropriate e-mail and internet communication. No member of the School community will do anything that compromises the security of the information held by the school

26. If a security incident is discovered, you must immediately report to the Business Manager or if they are involved the Headteacher providing as much information as possible.

27. A full record of the incident will be kept, including an outcome report. Care must be taken to comply with the timescales and escalation processes prescribed by the appropriate procedure that relates to the incident.

28. The School will keep a log of all incidents that are considered to be a breach of this policy to be analysed and inform future development. It will endeavour to safeguard against all risks although they may never be completely eliminated.

29. All users of the School's ICT facilities must keep their school account details secure and not share with other users. A user must log out of any device when they have finished using it.

Records Management

30. The School will ensure that it is responsible for the management of information to ensure secure access, effective retention, destruction and preservation of personal data.

31. The School will maintain records in line with legal requirements and best practice as recommended by the retention guidelines provided by the Records Management Society.

32. The School will review its historic records annually to ensure document retention complies with the guidelines

33. Personal data must not be stored on personal devices or on equipment not provided by the School.

34. The School does not permit the archive storage services of a commercial provider.

35. If emails are to be used as a record they must be printed/ scanned and stored with other records.

36. Emails are disclosable under FOI and DPL

Confidentiality

37. The human right of privacy must be respected. All communication of information must be dealt with, with sensitivity and discretion. Confidentiality can never be guaranteed in particular when safeguarding issues arise

38. The School will have rules for students and staff. The current rules for students are now set out in Appendix 1. These may be varied from time to time at the discretion of the Headteacher. Changes will be recorded in this section of the Policy.

E Safety

Introduction

39. We aim to ensure that students and staff are protected while using digital technologies at the School. The School is committed to including digital technologies, in particular, internet use, in our curriculum. In so doing, we recognise the inherent risks posed by this useful teaching and learning tool in exposure to inappropriate content and inappropriate contact from other children and adults. It also provides an opportunity to engage in unacceptable behaviour, both online and offline. The term digital technologies will include computers, tablets, laptops and mobile devices. The term digital technologies also includes all forms of electronic communication. This policy applies to all equipment using the School's network.

Internet

40. In order to keep staff and students safe online, and for them to learn how to keep themselves safe online, all students and staff should be aware of relevant skills and strategies needed to ensure internet safety. These will be embedded in our curriculum.

41. E safety will depend on our policies being properly implemented at all levels of the school community, a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and the effective teaching and training about digital technology use.

42. The School's internet system, and access to it, is specifically designed for staff and student use and filtering is appropriate for their use.

43. Students will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons. Students will be taught what internet use is acceptable / unacceptable. Teachers should be vigilant on safe use during internet based lessons. Teachers should use their professional judgement regarding what internet functions are appropriate for their lesson.

44. An agreed 'Acceptable Use of ICT' set of rules is displayed at the start of each academic year and is available each time a student accesses the internet. It is also available in the school planner.

Network

45. The Sandon School uses Virgin broadband via the London Grid for Learning with the appropriate firewall and safety filters. The security of the School's information systems and ICT system capacity will be reviewed regularly. The School's virus protection will be regularly updated by the London Grid for Learning. There are

procedures in place for virus protection to be installed and updated on all equipment identified by the Network Manager. This will include laptops used by staff or students issued by the school. This may also be used by a member of staff's own devices to avoid the transfer of virus between home and school.

Risk Management

46. Students should be taught about the dangers involved in email/ electronic communications. This will include not revealing personal details about themselves or others in email or electronic communication unless essential and authorised by a member of staff. Personal details will generally include full names, addresses, telephone numbers, e-mail addresses, names of friends, specific interests and clubs etc. Students should never, when using the facilities provided by the school, arrange to meet someone they have 'met' via email / online without the consent of the Headteacher who will require appropriate safeguarding measures such as the presence of a parent or a member of staff.

47. Students and parents will be informed of the risks inherent in using social media. Social media websites will not be accessible to students through the School's network.

48. The London Grid for Learning maintains a list of 'inappropriate' and 'banned' terms. The school's filtering system will, where possible, prevent access to inappropriate sites.

49. It is important to recognise that all emails sent to organisations or persons outside of the School are recognised as school communications and as such should be professional and will contain The Sandon School confidentiality notice

50. Only approved school emails accounts may be used via the school network for school related business.

51. Students should notify a member of staff immediately if they receive an offensive email and/or inappropriate material. Staff will notify a member of the Leadership Team.

Website

52. The Headteacher has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. Procedures will be in place for authorising the uploading of any content onto the School's website. No personal information or personal contact details will be published on the School's website. This extends to the use of students' full names. The school address, email and main telephone number should be the only contact information available to website visitors. Any images used should be carefully chosen with safeguarding in mind and it is advisable that students are not easily identifiable in images. Students' names should never be used in conjunction with their photograph on the website. The school will ensure that images chosen are not those where parents have refused permission.

Communication outside of the school

53. No communication should express views or opinions that could be construed by a third party as an official comment of the School without the authority of the Headteacher or the Chair of Governors.

Compliance and Review

54. The Governing Board will ensure that the School complies with all appropriate legislation and guidance on Information Communication Technology and E Safety and that this policy and all related procedures, statements and rules are implemented and monitored.

55. All members of the school community including parents, will be made aware of, and given guidance on, Information Communication Technology and E Safety, and support the School in this respect.

56. This policy has been developed in consultation with all stakeholders. It will be well publicised. It will be reviewed at least every three years. It was adopted by the Governing Board on 2 July 2018.

Appendix 1

Acceptable Use of ICT Rules - Students

We use school computers and Internet connection for teaching and learning. These rules will help us to be fair to others and keep everyone safe.

Using the school network, Internet, computers, laptops and all other devices

- When accessing the school network, I will use only my own authorised account details which I will keep secret and will not give to another person.
- I will log out of any device when I have finished using it.
- I will use the Internet, computers, laptops and other devices for schoolwork and homework which is appropriate for my education. If I wish to use them for any other purpose, I will check with an appropriate person first.
- I will not use the school's equipment or systems for accessing, storing or distributing anything that could be deemed inappropriate, a computer misuse offence or bring the school into disrepute.
- I will write emails carefully and politely. As messages may be forwarded, I understand that e-mail is best regarded as public property and that I am responsible for all emails I send and for contacts made. I understand that a displayed notice will inform students and staff of the school's disclaimer and confidentiality notice with regard to emails sent via the school email system.
- I understand that some emails, email attachments and external devices may contain harmful materials and computer viruses which may seriously affect the School's IT facilities. If I am unsure at any time, I will check with an appropriate person.
- I understand that anonymous messages and chain letters must not be sent and that the use of chat rooms is not allowed.
- The use of social media and on-line file sharing networks is not allowed using the School's network.
- I understand that, data protection and intellectual property rights such as copyright must be respected.
- I will not take any food or drink near any computers or IT equipment.
- I understand that if I bring my own equipment into school, these rules apply equally to any device.
- I will not link any hardware device to the computer nor install any software, without permission from the ICT Network Manager.
- I am aware that the School may check my computer files and may monitor the Internet sites which I visit**.**
- I will report any inappropriate content on the Internet or anything I see that I am concerned about when using the computer to an appropriate person.

I understand that irresponsible use may result in the loss of computer and/or Internet access and that disciplinary measures may be a consequence of a breach of these rules