



# All Saints Anglican School

Growing through Grace; Learning through Love

## Acceptable Use Agreement

Below are the conditions All Saints students are expected to adhere to when using any school owned or student owned device.

### 1 ACCEPTABLE COMPUTER AND INTERNET USE

Students will:

- 1.1 Not create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security.
- 1.2 Not bring any network connectivity device to the School that bypasses the School's internal control systems. This includes 3G/NextG/4G-type devices that connect to the One-to-One device either by plugging in or by connecting wirelessly.
- 1.3 Not disable settings for virus protection, spam and filtering that have been applied as part of the School's systems.
- 1.4 Ensure that communication through internet and online communication services is related to learning.
- 1.5 Keep passwords confidential and change them when prompted or when known by another user.
- 1.6 Use passwords that are not obvious or easily guessed.
- 1.7 Never allow others to use their personal school account on the device allocated to them.
- 1.8 Promptly report to the IT Department if they suspect they have received a computer virus or spam (unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.

Students will never send or publish:

- 1.9 Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- 1.10 Anything that is threatening, bullying or harassing towards another person or makes excessive or unreasonable demands upon another person.
- 1.11 Sexually explicit or sexually suggestive materials or correspondence.
- 1.12 False or defamatory information about a person or organisation.

Students will:

- 1.13 Ensure that personal use is kept to a minimum and internet and online communication services are generally used for curriculum and educational activities.
- 1.14 Not use of unauthorised programs or intentionally download unauthorised software, media or music that is not associated with learning.
- 1.15 Never damage or disable computers, computer systems or networks of the School.
- 1.16 Immediately report any damage that may have occurred their Senior School One-to-One device, to their classroom teacher or IT Helpdesk.
- 1.17 Ensure that (IT or Computer) services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- 1.18 Be aware that all use of internet and online communication services can be audited and traced to the accounts of specific users.

## **2 PRIVACY AND CONFIDENTIALITY**

Students will:

- 2.1 Never publish or disclose the email address of a staff member or student without that person's explicit permission.
- 2.2 Not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- 2.3 Ensure privacy and confidentiality are maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

## **3 INTELLECTUAL PROPERTY AND COPYRIGHT**

Students will:

- 3.1 Never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- 3.2 Ensure that permission is gained before electronically publishing users' works or drawings.
- 3.3 Always acknowledge the creator or author of any material published.
- 3.4 Ensure any material published externally to the School, including on the Internet:
  - 3.4.1 Has the approval of the Headmaster or their delegate and
  - 3.4.2 Has appropriate copyright clearance.
- 3.5 Misuse and Breaches of Acceptable Usage

Students will be aware that:

- 3.6 They are held responsible for their actions whilst using internet and online communication services.
- 3.7 They are held responsible for any breaches caused by them allowing any other person to use their school computer account to access internet and online communication services.
- 3.8 The misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

## **4 MONITORING, EVALUATION AND REPORTING REQUIREMENTS**

Students will report:

- 4.1 Any internet site accessed that is considered inappropriate.
- 4.2 Any suspected technical security breach involving users from outside the School.

Students also understand that:

- 4.3 In cases involving either school equipment or the use of network services, authorised school staff members are able to track and view communications including the content and transport information of email, social network service messages and other forms of electronic communications as required.
- 4.4 Authorised staff may inspect Senior School One-to-One devices and any other device that students bring to the School in order to audit digital files for inappropriate content, hazardous viruses, other malware and illegal software.
- 4.5 All material on the One-to-One device is subject to review by authorised School Staff.