INTERNET AND INFORMATION TECHNOLOGY USER POLICY – PART A

STUDENTS ONLINE - ACCEPTABLE USAGE POLICY

CONTENTS

Are you having difficulty understanding this document and would like a translator, please visit the College, or call us on 6207 5500. Translator services are provided free of charge by the Western Australian Department of Education.

INTRODUCTION

Mindarie Senior College, as part of the Department of Education, provides online services to students only for learning-related activities and makes every reasonable effort to educate and protect students from exposure to inappropriate online material and activities. The **Students Online - Acceptable Usage Policy** is an agreement that formally sets out the rules of use and expected behaviours for students using devices and online services as part of their education.

CONSENT AND ACCEPTABLE USE AGREEMENTS

Online Services provided to students in public Colleges require informed parental/carer consent and appropriate management.

By agreeing to the **Student's Rights and Responsibilities** in the College enrolment package, Mindarie Senior College students and their parents/guardians agree to the **Internet and Information Technology User Policy**.

STUDENT PERSONAL SECURITY

Parents/Carers will be aware of many incidents reported in the media regarding online safety. Personal information is easily tracked and harvested by those who know how, so it is important to keep as safe as possible while online.

Students should not reveal personal information, including names, passwords, addresses, photographs, credit card details and telephone numbers of themselves or others. Parents/Carers are encouraged to check the following sites online for further useful information.

- The eSafety Commissioner (eSafety) is Australia's independent regulator for online safety. This is the world's first government agency dedicated to keeping people safer online.

https://www.esafety.gov.au

- The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online.

www.staysmartonline.gov.au

- ThinkUKnow Australia is a partnership between the Australian Federal Police, Commonwealth Bank of Australia, Datacom, and Microsoft Australia, and delivered in partnership with all State and Territory police and Neighbourhood Watch Australasia. They develop resources and advice for parents, carers and educators, children, and young people to prevent online child sexual exploitation.

https://www.thinkuknow.org.au/resources-tab/parents-and-carers

RESPONSIBLE ONLINE PRACTICE

PERSONAL INFORMATION, PRIVACY AND CONFIDENTIALITY

Students should practice responsible security practices such as keeping their passwords secret and logging out of devices while they are not attended. Students are responsible for everything done using their College online services account and must inform staff if they think someone has interfered with or is using it.

Students should not publish or disclose the email addresses of staff or students without that person's explicit permission, and should take care when revealing personal information, including names, addresses, photographs, credit card details and telephone numbers of themselves or others.

PUBLISHING STUDENT IMAGES AND INFORMATION

Devices have the capacity to make digital images, both still and video. Unless appropriate permissions are sought, the taking of digital images is an invasion of personal rights. Under no circumstances can device computers be used to take or distribute digital images without both the expressed permission of the person whose image is being taken, and of College staff.

THIRD PARTY SERVICE PROVIDERS OF ONLINE APPLICATIONS

As a Department of Education College, Mindarie Senior College is required to identify online third-party services which hold students' personal information, confirm the Department has completed a risk assessment of the third-party service provider and complete appropriate parent notification or consent collection before using an online third-party service with students' personal information. The list of approved third party software is available on the College website under the Future Students tab.

The College recommends students limit the disclosure of personal or College information to third parties by avoiding subscribing to mailing lists or using their personal or College passwords when registering accounts.

STUDENT MISUSE AND BREACH OF ACCEPTABLE USE

APPROPRIATE USE OF ONLINE SERVICES

Students are to follow the instructions of teachers and only use online services for educational purposes. Students are required to avoid common distractions such as playing games during lessons and remain focused on the required learning activities.

GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

Access to Department of Education approved software may include generative AI components which can be utilised for educational purposes and within the confines of the MSC Assessment Policy and permitted Online Third Party Services. Students should not access unapproved generative AI systems, such as ChatGPT, due to privacy, content and safeguard concerns.

Assessment Policy

Third Party Services

CARE OF EQUIPMENT AND NETWORK INFRASTRUCTURE

It is expected that students take care of the equipment and infrastructure provided by the College. Students should take reasonable care not to damage or disable the hardware, software, systems or networks of the College, the Department of Education, or any other organisation.

RECEIVING INAPPROPRIATE MATERIAL FROM STUDENTS

Inappropriate content is content that is considered unsuitable or harmful to students. It includes material that is pornographic, racist, sexist, inflammatory, threatening, hateful, obscene, or abusive in nature or which promotes or encourages illegal activities or violence.

If students receive inappropriate or unwelcome online activity from fellow students or members of the public, they should immediately notify College staff. If necessary, staff will act in accordance with the Child Protection in Department of Education sites policy and procedures.

ACCESSING INAPPROPRIATE MATERIAL

Inappropriate content includes violent, racist, sexist, or pornographic materials, or content that is offensive, disturbing, or intimidating or that encourages dangerous or illegal activity. Students must not access, store, or send material that is considered inappropriate.

ONLINE IMPERSONATION

Students should neither attempt to find out other users' passwords, nor gain access to another user's network account, or impersonate any person or the school.

CYBERBULLYING AND HARRASSMENT

When using online services, students must behave in accordance with the College's policies and procedures regarding bullying and harassment. Students are not to bully or harass other students, staff or parents/carers and should be courteous and use appropriate language in all online communications.

CONSEQUENCES OF MISUSE AND BREACHES OF ACCEPTABLE USE

Student activity online can be monitored at any time at the College. Students will be held responsible for their actions while using online services and for any breaches caused by allowing any other person to use their online services account. Staff may request access to the device, including access to the internet browser history, logs, caches, files, and programs stored on the device. The misuse of online services may result in disciplinary action, determined by the Principal in accordance with the College's *Behaviour Management* policy.

Students may be held liable for offences committed using online services. Certain breaches which involve security and/or access violations may require the College to report them to the Australian Federal Police or State Police.