1. Purpose and Scope

The Acceptable Use of Information and Communications Technology (ICT) Policy sets out the standard of behaviour required by staff, contractors and volunteers when using the ICT resources of Christ Church Grammar School (the School). For the purposes of this policy ICT resources include but are not limited to the ICT network, infrastructure, applications, portals, cloud, mobile devices, internet, storage, email, telecommunications, printers, photocopiers and video conferencing equipment.

The purpose of this policy is to:

- Outline the general obligations and responsibilities of staff, contractors and volunteers in relation to the acceptable use of ICT resources across the School, including reasonable personal use
- Prevent misuse of ICT resources and minimise the risks associated with unethical behaviour
- Describe the access, monitoring and record keeping in relation to ICT resources, required by staff
- Protect the various data repositories of the School from the risks associated with misuse
- Identify the consequences of breaching this policy

All Christ Church Grammar School staff, volunteers and contractors who are provided with School supplied devices and/or access to the School's systems and/or network are bound by the provisions of this policy. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity. Individuals who breach the policy risk disciplinary action being taken against them.

2. Definitions

Confidentiality – the treatment of information which an individual has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission

Data – the term 'data' generally refers to unprocessed information, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. In this policy the terms 'data' and 'information' have been used interchangeably and should be taken to mean both data and information.

Information security – the practice of protecting information/data from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

Malware – software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

Minimal additional expense **–** expense associated with normal wear and tear or the use of small amounts of consumables

Password – A secret word or string of characters that is used for user authentication. Many two factor authentication techniques rely on password as one factor of authentication

Personal information – information or an opinion, whether true or not and whether recorded in a material form or not, about an individual, whether living or dead (a) whose identify is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particulars such as a fingerprint

Personal use – activity that is conducted for purposes other than accomplishing official duties

Social Media are defined as a group of internet-based applications which allow individual users/organisations to create, share and exchange user-generated content in online communities. Social media tools include but are not limited to the following:

- Social networking sites – Facebook, LinkedIn, Google
- Video/Photo Sharing sites – YouTube, Flikr, TikTok, Instagram, Vimeo
- Micro-Blogging sites – Twitter, Yahoo Buz, Meme
- Weblogs – corporate, personal or media blogs published through tools such as WordPress and Tumblr
- Forums and discussion boards – Whirlpool, Yahoo Groups, Google groups, Discord
- Instant message – Group SMS, WhatsApp, Facebook Messenger, WeChat
- Vod and podcasting – Spotify

Social Networking and social media are overlapping concepts, but social networking is usually understood as users building communities among themselves while social media is more about using social networking sites and platforms to build an audience.

3. Policy Principles

3.1 General provisions, obligations and responsibilities for the use of ICT resources

Staff using Christ Church Grammar School issued devices are subject to the ICT Asset Agreement governing the ownership, use and care of the asset.

All staff, contractors and volunteers must use ICT resources in a professional, responsible and ethical manner. Accordingly, these resources are not to be used

- To circumvent established information security procedures
- For any unlawful, illegal, malicious or improper purpose

- To store, transmit, publish, display or communicate/distribute/post material, which is obscene, defamatory, offensive, abusive, indecent, sexually explicit, threatening, discriminatory on the basis of race, religion, colour, age, sex, disability, ethnicity or gender orientation, related to terrorist activities, otherwise unlawful or unauthorised or violates any law or regulation
- To knowingly transmit a computer virus or other malware
- To access without permission, another staff member's ICT resources or damage the same
- To infringe the School's intellectual property rights or release commercial in confidence material
- To disclose private or confidential data or look up data in a School system in relation to a relative, friend or person associated with the School for purposes which are unrelated to your official duties
- To harass or menace any person
- To conduct, maintain or promote a personal private business, use for profit or gain
- To provide comments to journalists, politicians, lobby groups, endorsement of products outside fund-raising activities other than authorised in the course of your official duties
- To interfere with any individual's reputation, employment or other obligations
- To send bulk emails (without express permission), collect or harvest email addresses of others for the purpose of sending unsolicited emails or for sharing with external parties, or for illegal activities
- To create, send, or alter in any way the contents of emails for the purpose of hiding, obscuring or deleting the source of the message or making the message appear to come from someone other than the sender
- To breach any laws or infringe any third-party rights

Staff are required to minimise the risk associated with the misuse of ICT resources by:

- Keeping passwords confidential and by not using the logons and passwords of others
- Changing passwords if anyone else may know them
- Activating the screen saver or locking the system when away from workstations
- Logging out of systems when use is finished
- Not sharing devices with friends, family or non-approved staff members
- Not leaving devices in vehicles unattended
- Reporting lost or stolen devices to ICT Support as soon as possible and if stolen, lodging a report with the WA Police

3.2 Electronic communications

When communicating using the School's ICT resources staff are expected to act in a manner that reflects the school's values, views, and ethos. As a minimum staff are expected to:

- Maintain professional standards including spelling check, grammar check and compliance with all statutory obligations
- Adhere to the School's current style guide for communication including signatures, colours and fonts
- Use only school provided communications technologies e.g. email, Nexus or MS Teams when communicating with students, establishing any teacher-student collaboration or information distribution
- Respond to parents withing 24 working hours

3.3 Social Media and Social Networking

3.3.1 School Social Media Sites

Christ Church Grammar School uses social media tools to communicate with stakeholders including current and prospective parents and other interested parties. To maintain and grow the Christ Church brand, these tools are actively managed, and the requirements set out below are to be strictly followed:

- Authorisation from the Principal / Director of Communication and Engagement is required to set up a School social media account
- Communication to the school community will include a statement of purpose and that the objective is to share school communications – not to raise complaints
- Only authorised staff can publish content on the specific social media site with respect to which they have received authorisation
- Holders of site administration rights are responsible for uploading content, monitoring interactions on the site and taking down inappropriate posts

All queries and requests for advice on the use of the School's Social Media sites must be addressed to the Director of Communication and Engagement.

3.3.2 WhatsApp or other social media for year groups

Where WhatsApp or equivalent is used by the parents of students in a year group they are required to adhere to Guidelines set out in Appendix A to the Parents Code of Conduct.

3.3.3 External Social Networking Sites

Staff will not:

- Initiate online friendships with Christ Church Grammar School students and/or students from other schools
- Accept invitations from Christ Church Grammar School and non-Christ Church Grammar students as friends

- Discuss students or colleagues online
- Comment on or criticise school policies and/or personnel

3.4 Reasonable personal use of ICT resources

Reasonable personal use of ICT resources is permitted where ICT resources are already provided for work purposes, and this does not result in loss of productivity, does not interfere with official duties or result in more than minimal expense to the School. For example, this could include making a few photocopies, printing out a few pages of material, making an occasional brief personal telephone call, infrequently sending a personal email message, and limited use of the internet.

3.5 Compliance Monitoring

All electronic communication exchanged via the school's communication infrastructure remains the property of the School. The School has established processes to manage and monitor compliance with this policy. Whilst systematic and ongoing surveillance of staff member emails and internet access logs does not occur, authorised ICT staff may monitor or investigate staff use of the School ICT network systems and resources. This will occur to confirm compliance with the requirements of this policy and to investigate possible incidents of breaches of security, unauthorised access, or a breach in confidentiality. Unauthorised access, use and disclosure of confidential data will be deemed to be misconduct and will lead to disciplinary action.

3.6 Disclaimer

Christ Church Grammar School makes no warranties of any kind, whether express or implied, in relation to the electronic communication system.

The School will not be liable for any loss incurred by a person who provides personal information, including bank and/or credit card details over the internet or via email.

4. Related Policies and Resources

School Education Act 1999
School Education Regulations 2000
The Teachers Registration Act 2012
Corruption and Crime Commission Act 2003
Human Rights and Equal Opportunity Commission Act (1986)
Western Australian Equal Opportunities Act (1984)
Work Health and Safety Act 2020(WA)
Child Safety and Wellbeing
Child Protection and Mandatory Reporting
Code of Ethics
Code of Conduct Staff, Volunteers, Contractors
Parents Code of Conduct
Privacy Policy
Visual Identity Style Guide