Fact sheet: Internet Guidelines in the National Catholic Safeguarding Standards

Leadership, monitoring & improvement

STANDARD 8: Safe physical and online environments

Physical and online environments promote safety and contain appropriate safeguards to minimise the opportunity for children and adults to be harmed.

Criteria 8.2

The online environment is used in accordance with the entity's Code of Conduct and Safeguarding Policy.

Indicators

8.2.1 Personnel access and use online environments in line with the Code of Conduct, Privacy Act and relevant communication protocols.

8.2.2 The online environment is monitored, and breaches are managed in accordance with disciplinary procedures, or other relevant policies and reported to the leadership.

Standard 8 outlines our obligations to ensure safe physical and online environments.

Q: Why is internet filtering important?

Internet filtering is a fundamental safeguarding tool that strengthens protective safeguarding measures.

- Content filtering is the process of managing user access to enterprise-approved websites and by blocking them based on pre-determined security policies. Some web filtering tools are built into computers, devices, software, and streaming sites. They are used as a protective measure for organisations and individuals to prevent malware attacks or pose a risk to internet users.
- **Content filtering is a process that manages or screens access to specific emails or webpages.** The **goal** is to block content that contains **harmful information**. Organisations

use content filtering tools to **bolster security** and enforce corporate policies around **information system management**, such as when filtering social networking sites.

- Content filtering prevents access to content that could **pose a risk** to internet users. It blocks access to content deemed **illegal, inappropriate, or objectionable**. For example, it allows individual internet users to protect children from **exposure to graphic or improper material.** It also enables an organisation to **block access to pornographic content**, which, when left unmitigated, could lead to **sexual harassment c**laims, or **professional standards violations**.

- Content filters also allow organisations to block access to sites known to carry **malware**, protecting their data and users from **malicious activity** in the process. For example, Domain Name System (DNS) filtering can limit and block the threat of **internet-borne malware** and **reduce the remediation time** and workload necessary if malware penetration occurs. Firewalls that contain content filtering features can also **scan and scrutinize webpages to monitor for threats**. User knowledge about cyber safety can make a significant difference in the effectiveness of attacks and limit the chances of users visiting risky sites.

- Cyber criminals increasingly develop new, more sophisticated ways of **illegally accessing networks and stealing data**. **Exploit kits** contain code that enables a malicious actor to **attack web browser vulnerabilities through extensions and plugins.** This can lead users to unknowingly visit malicious websites, which may **trigger a malware download.** Content **filters can identify an exploit kit** and block access before it triggers a download.

Q: Why should we NOT use gmail /hotmail or similar addresses?

ACSL strongly recommends that all Church related activities are managed through domain email addresses as a safeguarding risk mitigation measure. These can be generic e.g. sacramentalprogram@stthomas.com or admin@stthomas.com

There are several reasons why it is an unsafe practice to use these public addresses for Church related activities.

- **Privacy:** Generic email addresses such as gmail, Hotmail, yahoo etc are not secure and easily hacked. Unless an individual has set up a corporate G Suite account in Google, your free gmail account is capturing and analysing data (that's the real price you are paying).
- **Chain of ownership of information:** this is especially important for security as well as productivity. When several people are involved in Ministry and are using personal email addresses, systematic information management can be lost, or inadvertently shared with others.
- **Chain of Evidence:** as a safeguarding protective measure, having a chain of evidence in relation to allegations and complaints is very important. These should not be on personal accounts but saved securely within the organisation. This evidence is subject to subpoenas or requests for information by police child protection services.

Q: What about Social Media and websites?

- It is important to make sure your website is hosted on a paid, secure site and has its own domain name (e.g. www.stthomas.com.au) rather than a free site such as Wix or Wordpress. This is because free sites are very easy to hack, divert, or embed malware.
- There should always be two administrators of any website, Facebook page or social media. This is to ensure that the content is moderated, and safeguarding settings and policies are adhered to e.g. Preventing comments from being posted on websites without approval, preventing unknown actors to post comments to a Facebook page or to share posts.

Q. What is the guidance about using photographs

- There is technology that can be used by potential abusers to track the meta data attached to photographs to discover the location, or to use AI to find other photographs of the same person to track them down.
- Always be conscious about the photographs that are posted to your website or social media.
- You may not be aware that a child captured in a photograph is subject to a child protection order.
- At a community event, always ask permission for photographs to be taken, and indicate where they may be used.
- Do not use them without permission given for their use**. It is illegal**.
- If taken on a personal device, they should be deleted as soon as possible.