# DIGITAL USE POLICY

## De La Salle District of Australia, New Zealand, Pakistan and Papua New Guinea (ANZPPNG)

Issue date: August 2020
Review date: August 2021

## 1.0 PURPOSE

This policy has been developed to ensure that across the ANZPPNG District engagement in digital media and the use of technology is safe, accurate, appropriate and as much as possible accessible.

It is acknowledged that online platforms are valuable tools with regard to education and communication. They provide a range of means for enabling interaction and the provision of services.

However, the importance of maintaining safe online environments in the promotion of the safety and well-being for all, especially children, young people and adults at risk is of paramount importance.

Therefore the District is committed to:

- Maintaining appropriate security and monitoring;
- Educating personnel on online safety and appropriate on-line behaviour; and
- Protecting the privacy of those subject to the policy in balance with the obligation of the District to fulfil safeguarding commitments.

## 2.0 SCOPE

This Policy applies to all personnel across the District including, employees, volunteers and religious, including those religious who are no longer in active ministry. It also applies to anyone engaged within Lasallian Ministries under contract.

The Policy applies to all personnel in their engagement in the online environment including when using internet, email, social media and devices including desktop and mobile.

The Policy recognises the breadth of the District and that personnel may be employed or directly connected to the District or Lasallian Ministries and related entities which may have their own policies for the use of internet, work provided device, as well as email and other internet and digital services.

## 3.0 PRINCIPLES

This Policy seeks to recognise the breadth of circumstances, both for Lasallian Ministries and individuals, and the different contexts across the District to which this policy will apply.

Whilst not an exhaustive list, these principles provide a broad framework for the application of this Policy. This policy is strongly aligned with the District Safeguarding Policy and the District Code of Conduct.

This policy:

- Is founded on the fundamental principle to protect children, young people and adults at risk and that this obligation is shared by all across the District
- Aims to deliver a safe environment for all across the District to use the internet, devices and to engage in the online environment with adequate protections and security
- Places an obligation on all for the appropriate use of resources
- Protects the privacy and security of all across the District
- Clearly identifies what is inappropriate use
- Outlines how breaches will be managed including in workplace investigations
- Reinforces that social media/online activity should always reflect Lasallian Values and respect for human dignity.

## 4.0 RESPONSIBILITIES

The District and Lasallian Ministries have a responsibility to ensure a safe environment for all (end users and personnel) whenever they are using internet services, including social platforms and /or devices provided by the District.

Such responsibility includes:

- The provision of secure internet services with appropriate security in place including firewalls;
- Ensuring devices such as mobile phones and laptops provided are equipped with appropriate security applications to protect users from external and malicious threats; and
- Ensuring compliance with all relevant laws in respect of the use of Internet services and devices including but not limited to safeguarding, privacy, and data protection.

Personnel covered by this policy have a responsibility to act lawfully and comply with all relevant legislation when using the internet, devices and engaging in online environments.

The viewing, downloading, sharing and/or production of child exploitation materials, grooming of children, young people and adults at risk are all criminal offences and any such unlawful activity detected will be reported to the Police.

It is expected that those involved in the Lasallian Mission will uphold the Principles at all times and under all circumstances regardless of who provides the device or internet connectivity.

## 5.0 SOCIAL MEDIA

Any social media activity undertaken should always reflect Lasallian Values and respect for human dignity.

Personnel who participate in social media in their personal capacity should be aware of their professional role and the potential for their personal views to be associated with their professional responsibilities.

Personnel are expected to be aware of and recognise their legal obligations in respect of social media applications are the same as if they were engaging non-digital interactions and activities. Accordingly, confidential, proprietary or privileged information should be never posted or published.

At all times professional boundaries should be maintained and as such personnel should avoid accepting or requesting students or young people engaged within Lasallian Ministries as 'friends'.

Content that violates the Code of Conduct should never be shared.

Personnel should recognise that social media platforms are public irrespective of the privacy setting selected and that any content has permanence.

Personnel should refrain from posting or sharing any content which may breach the District or Lasallian Ministries Codes of Conduct.

## 6.0 DISTRICT SUPPLIED DEVICES

The District provides devices including computers, laptops and other devices for work on behalf of the District.

Personnel are expected to use the device/s appropriately and with consideration for the purpose for which it is provided.

Devices have protection software installed to prevent virus, malware and ransomware. Web security will also be installed to protect devices when they are used remotely including web filtering and application control which blocks inappropriate web activity preventing access to inappropriate or illegal content by blocking websites and content related to criminal activity, extreme violent content, pornography and adult content and any download identified as high risk.

Web and internet activity on District devices is monitored and any activity that is detected and may be inappropriate, is reported to the Office Manager.

## 7.0 PRIVATE / INDIVIDUAL DEVICES

Personnel should note that the use of personal devices does not relieve them from their obligations in respect of meeting the relevant laws of the jurisdiction in which they are located.

Users of private devices should also be aware that monitoring of and recording of their internet activities, such as the retention and collection of metadata by ISP providers to meet their legislated requirements, is commonplace.

The District provides Brothers with access to endpoint protection for their private devices which Brothers are strongly encouraged to install.

## 8.0 VIRUSES / SPYWARE

Viruses and spyware present serious threats to information management/computer systems and can result in the theft and / or loss of data, disruption and disabling of IT systems and exposing the District and Lasallian Ministries to serious threats.

All Internet services and devices provided by the District and Lasallian Ministries should be equipped with appropriate security applications such as firewalls and antivirus software to protect users.

Similarly any users of District or Lasallian Ministries provided internet or devices should not open emails and / or attachments from people that they do not recognise or do not know.

## 9.0 PASSWORDS

Passwords used to access web-based platforms and/or devices provided by the District and/or Lasallian Ministries should be sufficiently complex and not based on personal information such as birthdates, addresses and the like.

Passwords should not be shared and if the security related to a password or passwords has been or is considered to be compromised then this should be reported immediately.

Passwords should be regularly changed and using the same password across devices, applications and websites, should be avoided.

Consideration should be given to the use of Two Factor authentication where available for added security.

## 10.0 FILE SHARING APPLICATIONS / USE OF CLOUD BASED STORAGE

The District provides a secure File Server which houses and protects important documents and materials stored.

Record management is critical to ensuring the accuracy of records and in the management of District business. All personnel are expected to follow record management procedures.

The use of other file sharing applications and /or cloud storage by individuals should be carefully considered particularly with respect to overall security as well as the security and protection of District documents and information.

## 11.0 USE IN A LEGAL AND ETHICAL MANNER

Use of the internet including social platforms and devices is subject to the full range of Government/s legislation as well as the policies and practices expected by the District.

Personnel need to ensure that use is at all times legal and ethical.

Examples of unlawful/inappropriate use include (but not limited to):

- Uploading, downloading, sending, receiving, producing or sharing of child exploitation material
- Using the Internet, social media or any other application to groom or solicit a child
- Viewing, sending and or receiving obscene or pornographic material
- Abusing, threatening, vilifying, defaming, harassing or discriminating against others
- Communicating violent messages or material
- Racist or other offensive communications
- Any illegal activity such as copyright infringement and or the illegal downloading of materials

## 12.0 MONITORING

The District protects security and privacy for users through the use of firewalls as well as monitoring networks for security issues in a number of ways.

This includes:

- Protecting the District Network from internet based threats with a firewall as well as Intrusion detection software. This protects documents and users on the network.
- Provides secure access – including Virtual Private Network (VPN) – for both Brothers and Personnel to access the file server in a secure fashion.
- Active web filtering across the network preventing any access to inappropriate or illegal content by blocking websites and content related to criminal activity, extreme violent content, pornography and adult content and any download identified as high risk.
- Active prevention of high risk online behaviour including VPN chatrooms, Bitcoin proxies and other proxies.

Personnel who use District resources should be aware that the District does monitor individual usage (including emails, internet, hard drives, networks and software) on a continuing basis for the limited purpose of ensuring compliance with security.

The District would normally only access records when;

- It reasonably suspects than an individual is not complying with the policy or other District polices; or
- When it is required to for legal proceedings or as required by law; or
- For IT security purposes (to protect networks).

Personnel should be aware internet use is also subject to monitoring and data collection by jurisdictions including retention of metadata and other records.

## 13.0 BREACHES

The District takes non-compliance with this policy seriously. If any user breaches the standards of use it may result in formal disciplinary action. Temporarily suspending the authority or access of a User to any system may also be applied pending an investigation into suspected breaches.

In the event of someone inadvertently breaching, i.e. clicking on a link which contains inappropriate content, or if they believe there password/s have been comprised, they are to advise their immediate Manager/Supervisor as soon as possible.

All personnel have an obligation if they become aware of possible or repeated breaches of this policy to report them immediately to the Head of the relevant Lasallian Ministry.

Penalties associated with violations of this policy will depend upon the severity of the breach.

If the District becomes aware of any suspected and or proven criminal conduct or breaches related to the safeguarding of children, young people and adults at risk, the District will report such to the Police or relevant authority.

## 14.0 REVIEW

This policy will be reviewed on an annual basis.

## 15.0 RELEVANT POLICIES AND DOCUMENTS

This Policy exists alongside a number of other relevant policies and documents.

- District Safeguarding Commitment Statement
- District Safeguarding Policy
- District Code of Conduct
- District Risk Management Plan
- National Catholic Safeguarding Standards

## 16.0 STATUS

This policy is approved by the Brother Visitor and is to be considered a mandatory document for all Lasallian Ministries in the District. This policy will be reviewed on an annual basis.

# APPENDIX 1 : DEFINITIONS

### Firewall

protects (a network or system) from unauthorised access.

### Internet

a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

### Intranet

Internal and restricted site accessible to personnel / employees / volunteers of a specific organisation.

### ISP

Internet service provider.

### Private / Individual Device

Use of a privately owned / individual device for work purposes.

### Cyber Bullying and Harassment

Bullying or harassment carried out online, via mobile phones through calls and SMS messaging, through social media or networking sites to harass, intimidate or abuse someone.

### Digital / Electronic Messaging

Term encompassing all forms of digital and communication such as SMS, Text, internet messaging tools such as Skype or messaging applications such as WhatsApp.

### Email

Enables people to exchange documents, files or messages in electronic form. It is a system by which people can send and receive messages via computers or mobile devices.

### Hack

Illegal or unauthorised entry into a computer system, files, server, device, Application or the like.

### Smart Device / Phone

A smart device or phone has advanced computing capability and connectivity such as an iPhone, iPad, Tablet, Android Device and the like.

### VPN

A virtual private network, or **VPN**, is an encrypted connection over the Internet.

### Spyware

Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

### Download

Copy (data) from one computer system to another, typically over the internet.

## Metadata

A set of data that describes and gives information about other data.

## Multi-factor authentication

**Multi-factor authentication** is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

## Two- factor authentication

**Two-factor authentication** is a type, or subset, of multi-factor authentication.
It is a method of confirming users' claimed identities by using a combination of *two* different factors: 1) something they know, 2) something they have, or 3) something they are.

A good example of two-factor authentication is the withdrawing of money from an ATM where only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out.

Two other examples are to supplement a user-controlled password with a One Time Password (OTP) or code generated or received by an authenticator (e.g. a security token or smartphone) that only the user possesses.