Diocese of Wilcannia-Forbes

Protocol: Use of Technology and Social Media to Communicate with Children and Adults at Risk

This protocol outlines the Diocese's expectations of Employees, Volunteers, contractors, Clergy and Religious Appointees in relation to the use of social media and technology to communicate with and engage with Children and Adults at Risk.

Key Obligation

It is important to be respectful, transparent and responsible when using technology and social media to communicate with Children and Adults at Risk. The Diocese has zero tolerance for cyber-bullying or the posting or sharing of Intimate Images of Children and/or Adults at Risk.

1 Types of communication to which this protocol applies.

1.1 Social media

a) The *Online Safety Act 2021* defines a 'social media service' as an electronic service that enables online social interaction between two or more users and the posting or linking of material between users.

b) Generally, social media refers to web-based external, commercial, or media websites and applications used to connect with other people and maintain relationships and communities.

c) There are many types of social media platforms. Examples include Facebook, Twitter, Instagram, WhatsApp, Snapchat, Discord, Myspace, Bebo, Tik Tok and Xt3.

d) This protocol is intended to provide guidance in relation to communications with Children and Adults:

(i) via social media that take place on a 'one-on-one' basis; and

(ii) via open and transparent group communications such as public posts on official Diocesan Facebook pages or on the Diocesan Catholic Talk website.

1.2 Technology

a) People use technology to communicate in various ways including the use of email, internet browsing, text messaging, online chats, video conferencing, gaming, blogging and online forums, phone, mobile phone and on a variety of devices.

b) This protocol applies to all forms of technology.

2 Cyber-Bullying Material and Intimate Images

a) The *Online Safety Act 2021* provides a mechanism for the following persons to make complaints to the eSafety Commissioner if they believe that a Child and/or an Adult is the target of Cyber-Bullying Material provided through a social media service or the subject of an Intimate Image posted through a social media service:

(i) the Child;

(ii) the Child's parents or guardians; or

(iii) an Adult authorised by the Child to make a complaint on their behalf.

(iv) the Adult

(v) an Adult authorised by another Adult to make a complaint on their behalf.

b) The eSafety Commissioner has the power to investigate complaints and obtain any information or make any inquiries that it considers appropriate for investigating complaints. The eSafety Commissioner may then issue various notices on social media services, requesting or requiring the removal of Cyber-Bullying Material or Intimate Images.

c) **"Cyber-Bullying Material targeted at an Australian Child"** is:

(i) material provided on a social media service, relevant electronic service, or a designated internet service that an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Child residing in Australia; and

(ii) the effect is one that would be seriously threatening, seriously intimidating, seriously harassing or seriously humiliating to the Child residing in Australia.

d) **"Cyber-Bullying Material targeted at an Australian Adult"** is:

(i) Material provided on a social media service, relevant electronic service, or a designated internet service that an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult; and

(ii) The effect is that the material would be regarded as being menacing, harassing or offensive.

e) An **"Intimate Image"** is:

(i) material consisting of either a still visual image or a moving visual image that depicts or appears to depict:

A. a person's genital, anal or breast areas, whether bare or covered by underwear; or

B. a person in a state of undress, using the toilet, showering, bathing, engaged in a Sexual Act, or any other like activity; or

C. a person without particular attire of cultural or religious significance, that they consistently wear in public because of their culture, background or religion.

in circumstances in which an ordinary reasonable person would expect to be afforded privacy.

f) **"Non-consensual Intimate Image of a person**" is:

(i) Intimate Images of an Adult on a social media service, relevant electronic service, or a designated internet service that the person did not consent to.

3 Diocese's Policy and Procedure

3.1 General responsibilities of Employees, Volunteers, contractors, Clergy and Religious Appointees when using technology to communicate with Children and Adults at Risk

a) In the Parish and Agency context, Employees, Volunteers, contractors, Clergy and Religious Appointees **must**:

i) be respectful, polite, and considerate in all communications with Children and/or Adults at Risk;

ii) communicate in a manner that is consistent with their role and responsibility within or in relation to the Parish or Agency;

iii) be transparent and identify themselves by using their real name;

iv) respect the privacy of others and ensure that information is not transmitted or published that should not be made public;

v) subject to the exceptions at (vii) below, avoid communicating on an individual (one-on-one) basis with any Child ***unless*** they have the written consent of that Child's parent or guardian and have included the Child's parent or guardian in the communication; and

vi) subject to the exceptions at (vii) below, the exceptions seek to ensure that communication with Children is via face-to-face discussions, group communications and other means which are open and transparent.

vii) Exceptions:

A. In exceptional circumstances where there is a genuinely held concern about the safety or well-being of a Child, brief engagement via technology or social media may be appropriate in order to provide advice and support. However, this should only occur where advice and support is necessary on an urgent basis and should not involve prolonged engagement. Records should be kept of any engagement of this kind and parental consent to any ongoing technology or social media communications should be sought at the earliest possible time if it is safe and appropriate to seek that consent.

B. If a Child initiates contact via technology or social media seeking information about vocations and other practical aspects of Church operations, it is permissible to respond but only to the extent necessary to answer the specific request for information.

b) Employees, Volunteers, contractors, Clergy and Religious Appointees **must not**:

i) invite or accept invitations from Children they have met through the Diocese as "friends" on their personal social media site, e.g. their Facebook profile;

ii) interact with Children they have met through the Diocese on their personal social media site;

iii) communicate with a Child on a one-to-one basis by phone (including mobile phone and text messages) or email, unless the relevant Parish Priest or Agency Head has obtained the express, written consent of the Child's parent or guardian;

iv) send, post, share, or link any Cyber-Bullying Material targeted at a Child and/or Adult at Risk, Intimate Images of a Child or Non-Consensual Intimate Images of an

Adult. Use language or images that are inappropriate, e.g., material that is harassing, defamatory, bullying, threatening, sexually explicit, obscene, profane, illegal or otherwise offensive;

v) send to a Child or request from a Child image of a particular Child or Children in individual (one-on-one) communications ***even if*** there is written consent from that Child's parent or guardian allowing communication with them. If images of a particular Child or Children are received from a Child, they should be shown to a Parish Priest, Agency Head or a member of the Safeguarding Office in accordance with part 5 of this protocol, so that consideration can be given to whether any notification to an external authority is required. Images should then be deleted immediately thereafter.

4 Social Media Accounts/Platforms

a) All social media accounts/platforms connected to a Parish or Agency of the Diocese must have more than one administrator. The administrators of Parish or Agency social media accounts/platforms must be over the age of 18 years.

b) Parish Priest and Agency Heads are to be made aware of the content being posted to social media accounts/platforms that are connected to their Parish or Agency.

5 Reporting of Cyber-Bullying Material, Intimate Images, or other inappropriate comments or images

a) All Employees, Volunteers, Clergy and Religious Appointees must immediately notify the relevant Parish Priest or Agency Head if:

i) they become aware of any Cyber-Bullying Material or Intimate Images of a Child and/or Adult at Risk on Diocesan Facebook pages, the Diocesan Catholic Talk website or any other platform associated with the Diocese, its Parishes or Agencies;

ii) they become aware of inappropriate comments or images or material that could be considered Cyber-Bullying Material or Intimate Images, being exchanged between Children and/or Adults at Risk or between Children and/or Adults at Risk and any Employee, Volunteer, member of the Clergy or Religious Appointee;

iii) any inappropriate comments or images are directed to them by a Child and/or Adult at Risk;

iv) they become aware that another Employee, Volunteer, member of Clergy or Religious Appointee has otherwise acted in breach of the obligations listed in paragraph 3.1 of this protocol; or

v) they become aware of any conduct via technology or social media regarding a Child and/or Adult at Risk that should be notified to a Child's parents/guardians, Adult at Risk's carer and the eSafety Commissioner, or that is otherwise reportable to the NSW Police, NSW Office of the Children's Guardian or the Department of Communities and Justice.

b) The Parish Priest or Agency Head must immediately notify the Safeguarding Office, which will determine whether the matter is required to be reported to the NSW Police, NSW Office of the Children's Guardian or the Department of Communities and Justice, or otherwise dealt with.

c) Where a Child and/or Adult at Risk is associated with the Diocese, its Parishes or Agencies is the subject of Cyber-Bullying Material, Intimate Images or Non-Consensual Intimate Images (Adult) shared via social media, the Parish Priest, Agency Head and/or Safeguarding Office should work with the Child and/or Adult at Risk and/or their parents/guardians/carers (as appropriate), to make a complaint to the eSafety Commissioner.