Data Processing Agreement

This Data Processing Agreement ("Agreement" or "DPA") forms part of the Contract for Services, Terms and Conditions, Privacy Policy, and any other applicable written agreement between New World Solutions Pty Ltd, Clarence St, Sydney NSW 2000 ("New World Solutions", "Processor", "we", "us", or "our") and the congregation using the Services ("Congregation", "Controller", "you", or "your").

This Agreement governs the Processing of Personal Data by New World Solutions on behalf of the Congregation in connection with the Services, including NWS Desktop, NWS Mobile, NW Publisher, related synchronization services, sharing services, hosting services, support services, and any other online or connected services provided by New World Solutions.

This Agreement is complementary to the Privacy Policy, which describes our general privacy practices, service operation, security measures, Subprocessors, and related data protection information. If there is a conflict between this Agreement and the Privacy Policy in relation to the Processing of Congregation Personal Data by New World Solutions as Processor, this Agreement will prevail to the extent of the conflict.

The term of this Agreement follows the term of the Principal Agreement, unless this Agreement expressly states otherwise or unless obligations must continue after termination by their nature, including confidentiality, security, deletion, audit, data transfer, and legal compliance obligations.

Background

A. The Congregation acts as Controller in relation to Congregation Personal Data Processed through the Services.

B. New World Solutions acts as Processor when Processing Congregation Personal Data on behalf of the Congregation for the purpose of providing the Services.

C. The Congregation wishes to use the Services, and such use may involve the Processing of Personal Data subject to applicable Data Protection Laws, including the GDPR where applicable.

D. The Parties wish to set out their respective rights and obligations in relation to the Processing of Congregation Personal Data.

E. The Processor receives, stores, transmits, synchronizes, and makes available encrypted and obfuscated data strings received from the Congregation's local NWS Desktop or NWS Mobile software and makes such data available to other approved users within the same Congregation, subject to the Congregation's instructions, configuration, permissions, approvals, and use of the Services.

1. Definitions and Interpretation

Unless otherwise defined in this Agreement, capitalized terms used in this Agreement have the meaning given to them in the GDPR or other applicable Data Protection Laws.

1.1. “Agreement” means this Data Processing Agreement, including all schedules and attachments.

1.2. “Approved User” means a person approved, invited, authorized, configured, or permitted by the Congregation to access or use the Services, or to access data made available by the Congregation through the Services.

1.3. “Congregation Personal Data” means Personal Data Processed by the Processor on behalf of the Congregation in connection with the Services, including encrypted and obfuscated data strings received from local NWS Desktop or NWS Mobile software, and any limited Personal Data expressly described in this Agreement.

1.4. “Controller” means the Congregation, being the person or body that determines the purposes and means of Processing Congregation Personal Data.

1.5. “Data Protection Laws” means all data protection, privacy, electronic communications, and data security laws applicable to the Processing of Congregation Personal Data under this Agreement, including, where applicable, the GDPR, UK GDPR, Australian Privacy Act 1988 (Cth), Australian Privacy Principles, and any law implementing, supplementing, replacing, or amending those laws.

1.6. “Data Subject” means an identified or identifiable natural person to whom Personal Data relates.

1.7. “Data Transfer” means a transfer, disclosure, remote access, onward transfer, transmission, hosting, storage, or other making available of Congregation Personal Data from one country or jurisdiction to another, whether by the Controller, Processor, Subprocessor, Approved User, or other authorized recipient.

1.8. “EEA” means the European Economic Area.

1.9. “Encrypted and Obfuscated Congregation Data” means Congregation Personal Data received by the Processor from local NWS Desktop or NWS Mobile software in encrypted and obfuscated string form, where the Processor does not possess, store, derive, recover, or otherwise have access to the decryption keys required to read the plaintext contents.

1.10. “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.11. “Personal Data” has the meaning given to it in the GDPR or other applicable Data Protection Laws.

1.12. “Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

1.13. “Principal Agreement” means the Contract for Services, Terms and Conditions, account agreement, order, subscription, or other agreement under which the Congregation obtains access to the Services.

1.14. “Processing” means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

1.15. “Processor” means New World Solutions Pty Ltd when Processing Congregation Personal Data on behalf of the Congregation.

1.16. “Services” means NWS Desktop, NWS Mobile, NW Publisher, synchronization services, sharing services, hosting services, support services, account services, authentication services, diagnostic services, and related online, connected, or hosted services provided by New World Solutions.

1.17. “Shared Person” means a person invited, approved, or configured by the Congregation to use or access the Services, or whose First Name and email address are Processed for the purpose of invitation, access, identification, authentication, notification, or service availability.

1.18. “Subprocessor” means any third party appointed by or on behalf of the Processor to Process Congregation Personal Data on behalf of the Congregation in connection with the Services.

1.19. “Supervisory Authority” means an independent public authority established by a Member State under the GDPR, or any equivalent competent data protection, privacy, or regulatory authority under applicable Data Protection Laws.

1.20. References to “including” mean “including without limitation”.

1.21. References to a law include that law as amended, replaced, re-enacted, or supplemented from time to time.

2. Roles of the Parties

2.1. The Congregation is the Controller of Congregation Personal Data.

2.2. The Processor Processes Congregation Personal Data on behalf of the Congregation and only in accordance with this Agreement, the Principal Agreement, documented instructions from the Congregation, and applicable Data Protection Laws.

2.3. The Congregation is responsible for determining the purposes and means of Processing Congregation Personal Data, including determining what data is entered into local NWS Desktop or NWS Mobile software, what data is synchronized through the Services, what data is shared, which persons are approved to access data, and whether the Congregation has a lawful basis for such Processing.

2.4. The Processor does not determine the purposes for which the Congregation enters, uploads, stores, shares, synchronizes, or makes available Congregation Personal Data through the Services.

2.5. The Processor may Process limited Personal Data as an independent controller where necessary for its own business operations, including account management, billing, tax compliance, corporate records, legal compliance, service communications, and direct support interactions. Such Processing is outside the scope of this Agreement except to the extent required by applicable Data Protection Laws.

3. Processing of Congregation Personal Data

3.1. The Processor shall Process Congregation Personal Data only:

(a) to provide, operate, maintain, secure, support, and improve the Services;

(b) to receive, store, transmit, synchronize, and make available Encrypted and Obfuscated Congregation Data to Approved Users within the same Congregation;

(c) to process the First Name and email address of Shared Persons where necessary for invitation, identification, authentication, notification, support, or access to the Services;

(d) to process anonymous diagnostic data for service reliability, error detection, security, performance, and operational diagnostics;

(e) to comply with applicable legal obligations;

(f) to resolve disputes, enforce agreements, prevent abuse, investigate security issues, and protect the integrity of the Services;

(g) as otherwise expressly instructed by the Congregation in writing.

3.2. The Congregation instructs the Processor to Process Congregation Personal Data for the purposes described in this Agreement, the Principal Agreement, the Privacy Policy, and Schedule 1.

3.3. The Processor shall not sell Congregation Personal Data.

3.4. The Processor shall not use Encrypted and Obfuscated Congregation Data for advertising, profiling, marketing, data mining, or any purpose unrelated to providing,

securing, maintaining, supporting, or complying with legal obligations in relation to the Services.

3.5. The Processor cannot read, inspect, search, interpret, disclose, or use the plaintext contents of Encrypted and Obfuscated Congregation Data because the Processor does not possess, store, derive, recover, or otherwise have access to the decryption keys required to read such contents.

3.6. The Processor's role in relation to Encrypted and Obfuscated Congregation Data is limited to receiving, storing, transmitting, synchronizing, making available, and deleting encrypted and obfuscated strings in accordance with the Congregation's instructions and configuration.

3.7. Use of Congregation Sharing is optional and is enabled, configured, and controlled by the Congregation. The Congregation determines whether Congregation Sharing is enabled, which persons are approved to access shared data, which permissions apply, and which sharing server region is selected where such selection is made available by the Services.

3.8. Where Congregation Sharing is used, access is protected by authentication and authorization controls, which may include OAuth 2.0 authorization, access tokens, refresh tokens, Congregation ID, Congregation Sharing Password, email identification, device verification, and verification codes.

3.9. Access credentials are scoped to the relevant Congregation. Approved Users are not authorized to access encrypted and obfuscated data strings belonging to any other congregation.

3.10. Each Congregation is assigned a unique and obfuscated storage location for encrypted and obfuscated data strings. Access to that location is restricted to Approved Users who satisfy the applicable authentication and authorization requirements.

3.11. If the Congregation disables Congregation Sharing, the encrypted and obfuscated data strings stored for Congregation Sharing are deleted from the sharing server through the normal operation of the Services.

4. Documented Instructions

4.1. The Processor shall Process Congregation Personal Data only on documented instructions from the Congregation, unless required to do so by applicable law.

4.2. The Principal Agreement, this Agreement, the Privacy Policy, the Congregation's configuration of the Services, user permissions, sharing settings, support requests, account instructions, and written communications from the Congregation constitute documented instructions.

4.3. If the Processor is required by law to Process Congregation Personal Data other than in accordance with the Congregation's documented instructions, the Processor shall, to

the extent legally permitted, inform the Congregation of that legal requirement before Processing.

4.4. The Processor shall promptly inform the Congregation if, in the Processor's opinion, an instruction from the Congregation infringes applicable Data Protection Laws, unless the Processor is prohibited from doing so by applicable law.

4.5. The Processor is not required to assess the lawfulness, accuracy, completeness, appropriateness, or necessity of Congregation Personal Data entered, uploaded, synchronized, shared, or otherwise Processed by the Congregation, except to the extent expressly required by applicable Data Protection Laws.

5. Congregation Responsibilities

5.1. The Congregation is responsible for ensuring that it has all necessary rights, permissions, notices, consents, lawful bases, and authority required to collect, enter, store, synchronize, transfer, share, and otherwise Process Congregation Personal Data through the Services.

5.2. The Congregation is responsible for ensuring that Congregation Personal Data is accurate, relevant, lawful, and limited to what is necessary for the Congregation's purposes.

5.3. The Congregation is responsible for approving, configuring, reviewing, and removing Approved Users.

5.4. The Congregation is responsible for ensuring that Approved Users are authorized to access Congregation Personal Data made available to them.

5.5. The Congregation is responsible for protecting local installations of NWS Desktop and NWS Mobile, user devices, passwords, account credentials, local files, local backups, local exports, and local network environments.

5.6. The Congregation acknowledges that the Processor cannot prevent an Approved User from reading, copying, exporting, disclosing, or otherwise using data that the Congregation has authorized that Approved User to access.

5.7. The Congregation is responsible for determining whether any Congregation Personal Data constitutes special category data, sensitive information, confidential pastoral information, or other regulated information, and for ensuring that any such Processing is lawful and appropriate.

6. Processor Personnel

6.1. The Processor shall take reasonable steps to ensure that persons authorized to Process Congregation Personal Data are reliable and are subject to appropriate confidentiality obligations.

6.2. Access to systems used to provide the Services shall be limited to persons who require access for legitimate operational, support, security, legal, or administrative purposes.

6.3. Personnel access shall be restricted according to role, need, and purpose, taking into account the nature of the Services and the Processor's inability to read Encrypted and Obfuscated Congregation Data.

6.4. The Processor shall ensure that personnel authorized to Process Congregation Personal Data are informed of the confidential nature of such data and are required to protect it in accordance with this Agreement.

7. Security

7.1. Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of Processing, and the risks presented to the rights and freedoms of natural persons, the Processor shall implement and maintain appropriate technical and organisational measures designed to ensure a level of security appropriate to the risk.

7.2. The Processor's technical and organisational measures include, as applicable to the Services:

(a) encryption and obfuscation of Congregation Personal Data received from local NWS Desktop or NWS Mobile software;

(b) end-to-end encryption for Encrypted and Obfuscated Congregation Data, where the Processor does not possess, store, derive, recover, or otherwise have access to the keys necessary to read the plaintext contents;

(c) local generation and local storage of encryption keys, with such keys not transferred to, stored by, or made available to the Processor or the sharing server;

(d) symmetric encryption for Encrypted and Obfuscated Congregation Data, with 256-bit encryption keys derived locally using password-based key derivation, including Argon2id and SHA-256, and with a random and unique initialization vector and salt generated for each transferred item where applicable;

(e) encrypted transport security for data in transit, including TLS 1.2 or higher where supported, and no use of TLS 1.0 or TLS 1.1 for Congregation Sharing data transfer;

(f) authentication and authorization controls for Approved Users, which may include OAuth 2.0 authorization, access tokens, refresh tokens, Congregation ID, Congregation Sharing Password, email identification, device verification, and verification codes;

(g) access credentials scoped to the relevant Congregation, so that Approved Users are not authorized to access encrypted and obfuscated data strings belonging to any other congregation;

(h) unique and obfuscated storage locations for Congregations using Congregation Sharing;

(i) access controls designed to restrict access to systems, accounts, and administrative functions to persons who require such access for legitimate operational, support, security, or legal purposes;

(j) logical separation of Congregation data;

(k) use of Google Firebase and related Google Cloud infrastructure as the Processor's appointed infrastructure Subprocessor for hosted storage, authentication, serverless processing, synchronization, transfer, service security, diagnostics, and related service operation;

(l) use of selected sharing server regions where such selection is made available by the Services;

(m) measures intended to prevent unauthorized access, accidental loss, accidental disclosure, unauthorized alteration, or unauthorized destruction of Congregation Personal Data;

(n) service monitoring, operational diagnostics, and error detection designed to maintain the availability, integrity, and reliability of the Services;

(o) reasonable administrative controls over personnel, contractors, and Subprocessors who may have access to systems used to provide the Services;

(p) confidentiality obligations for persons authorized to Process Congregation Personal Data;

(q) controlled support access procedures;

(r) deletion controls allowing Congregation Personal Data to be deleted by the user at any time where such functionality is provided in the Services;

(s) automatic deletion of inactive data after 60 days;

(t) avoidance by the Processor of separate backup copies of Congregation Personal Data, except where transient technical replication, infrastructure redundancy, or temporary operational processing is strictly necessary for service operation and is not retained by the Processor as a separate backup copy;

(u) review and improvement of technical and organisational measures where reasonably appropriate having regard to the nature of the Services.

7.3. For Congregation Personal Data stored as encrypted and obfuscated strings using end-to-end encryption, the Processor cannot read or access the plaintext contents of such data. The Processor's Processing of such data is limited to storage, transmission, synchronization, availability, and deletion of encrypted and obfuscated strings.

7.4. The Congregation acknowledges that security of the Services also depends on the Congregation's configuration, user approvals, user devices, local NWS Desktop or NWS Mobile installations, passwords, account access controls, and the conduct of Approved Users.

7.5. The Processor shall take reasonable steps to evaluate, review, and, where appropriate, improve the effectiveness of its technical and organisational measures, having regard to the risk, the nature of the Services, and the Processor's role as Processor.

8. Subprocessing

8.1. The Processor uses Google Firebase and related Google Cloud Platform services as its only appointed infrastructure Subprocessor for the Services. This Subprocessor is used to provide hosted storage, authentication, serverless processing, synchronization, encrypted data transfer, service security, diagnostics, operational availability, and related technical infrastructure required for the Services.

8.2. The Processor does not appoint any other Subprocessor to store, host, synchronize, or make available Encrypted and Obfuscated Congregation Data, unless this Agreement is amended or the Congregation is notified in accordance with this section.

8.3. Firebase is provided by Google. Google's Firebase Data Processing and Security Terms identify Google LLC, Google Ireland Limited, or other Google-controlled entities as the applicable Google entity depending on the relevant agreement and circumstances.

8.4. Google's published Firebase and Google Cloud security information describes technical and organisational measures including physically secure data centres, redundancy, business continuity planning, internal access controls, personnel confidentiality obligations, incident response procedures, encryption technologies, HTTPS/TLS availability, and security measures for subprocessors.

8.5. Google states that Firebase services have completed ISO 27001 and SOC 1, SOC 2, and SOC 3 evaluation processes, and that some Firebase services have also completed ISO 27017 and ISO 27018 certification processes. Google Cloud Platform is also certified as ISO/IEC 27001:2022 compliant and ISO/IEC 27018 compliant.

8.6. The Congregation grants the Processor general written authorization to use Google Firebase and related Google Cloud Platform services as described in this section.

8.7. If the Processor intends to appoint an additional Subprocessor to store, host, synchronize, or make available Encrypted and Obfuscated Congregation Data, the Processor shall inform the Congregation of the intended addition or replacement. Such

notice may be provided by email, through the Services, through the Processor's website, through the Privacy Policy, or by another reasonable notification method.

8.8. The Congregation may object to the addition or replacement of a Processor-appointed Subprocessor on reasonable data protection grounds by notifying the Processor in writing within 14 days after notice is provided.

8.9. If the Congregation objects, the Processor shall use reasonable efforts to address the objection, which may include providing further information, changing the relevant Processing arrangement, or allowing the Congregation to terminate the affected Services where the objection cannot reasonably be resolved.

8.10. The Processor remains responsible for the performance of its directly appointed Subprocessors' obligations to the extent required by applicable Data Protection Laws.

9. Data Subject Rights

9.1. Taking into account the nature of the Processing and the information available to the Processor, the Processor shall reasonably assist the Congregation in fulfilling the Congregation's obligations to respond to requests by Data Subjects exercising rights under applicable Data Protection Laws.

9.2. The Processor shall promptly notify the Congregation if it receives a request from a Data Subject relating to Congregation Personal Data.

9.3. The Processor shall not respond to a Data Subject request relating to Congregation Personal Data except:

(a) on documented instructions from the Congregation;

(b) to confirm that the request should be directed to the Congregation; or

(c) where required by applicable law.

9.4. Where the Processor is required by applicable law to respond to a Data Subject request, the Processor shall, to the extent legally permitted, inform the Congregation before responding.

9.5. The Congregation acknowledges that the Processor may be unable to access, read, search, extract, correct, or produce the plaintext contents of Encrypted and Obfuscated Congregation Data because the Processor does not possess the decryption keys required to read such contents.

10. Personal Data Breach

10.1. The Processor shall manage Personal Data Breaches in accordance with applicable Data Protection Laws and its internal incident response procedures.

10.2. In the event of a Personal Data Breach affecting Congregation Personal Data, the Processor shall notify the Congregation without undue delay after becoming aware of the Personal Data Breach.

10.3. The Processor's notice shall include sufficient information, to the extent reasonably available to the Processor, to enable the Congregation to meet its obligations under applicable Data Protection Laws.

10.4. Such information may include, where available and applicable:

(a) the nature of the Personal Data Breach;

(b) the categories and approximate number of affected Data Subjects;

(c) the categories and approximate number of affected records;

(d) the likely consequences of the Personal Data Breach;

(e) measures taken or proposed to address the Personal Data Breach;

(f) measures taken or proposed to mitigate possible adverse effects;

(g) relevant contact information for follow-up.

10.5. The Processor shall provide information in phases where not all information is immediately available.

10.6. The Processor shall cooperate with the Congregation and take reasonable commercial steps, as directed by the Congregation and taking into account the nature of the Processing and information available to the Processor, to assist in the investigation, mitigation, and remediation of a Personal Data Breach affecting Congregation Personal Data.

10.7. Each Party shall bear the costs of investigation, remediation, mitigation, and related costs to the extent the Personal Data Breach was caused by that Party's breach of this Agreement.

10.8. Each Party shall bear the costs of fines, penalties, damages, or other amounts imposed by an authorized regulatory body, governmental agency, or court of competent jurisdiction to the extent arising from that Party's breach of its obligations under this Agreement.

10.9. Notification of a Personal Data Breach is not an admission of fault or liability by the Processor.

11. Data Protection Impact Assessments and Prior Consultation

11.1. Taking into account the nature of the Processing and the information available to the Processor, the Processor shall provide reasonable assistance to the Congregation with

data protection impact assessments and prior consultations with Supervisory Authorities or other competent data protection authorities where required by applicable Data Protection Laws.

11.2. The Processor's assistance shall be limited to Processing of Congregation Personal Data by the Processor and information available to the Processor.

11.3. The Congregation acknowledges that the Processor may be unable to provide information about the plaintext contents of Encrypted and Obfuscated Congregation Data because the Processor cannot read such contents.

12. Deletion or Return of Congregation Personal Data

12.1. Congregation Personal Data can be deleted by the user at any time where deletion functionality is made available in the Services. The Processor shall give effect to such deletion through the normal operation of the Services.

12.2. The Processor does not create backup copies of Congregation Personal Data and does not make additional copies of Congregation Personal Data except to the extent strictly necessary for the immediate technical operation, transmission, synchronization, security, or availability of the Services.

12.3. Inactive data is automatically deleted after 60 days, unless retention is required by applicable law, necessary to complete a user-requested action, necessary for security or abuse prevention, or otherwise expressly agreed with the Congregation.

12.4. Upon termination or cessation of the Services, the Processor shall delete Congregation Personal Data in accordance with this Agreement, the Terms and Conditions, and the Privacy Policy, unless applicable law requires continued storage.

12.5. Where the Congregation requires a copy of its data, the Congregation must export, download, retrieve, or request such data before deletion of the relevant account or data. Requests made after deletion may not be capable of fulfilment because the Processor does not maintain backup copies or separate retained copies of deleted Congregation Personal Data.

12.6. Where Congregation Personal Data is stored as encrypted and obfuscated strings, deletion means deletion of the encrypted and obfuscated strings held by the Processor.

12.7. The Processor is not able to decrypt, read, reconstruct, or return the plaintext contents of encrypted and obfuscated strings unless the Congregation or an Approved User provides the necessary plaintext or decryption capability.

12.8. Nothing in this section requires the Processor to delete data that it is legally required to retain, provided that any such retained data shall remain subject to the confidentiality and security obligations of this Agreement for so long as it is retained.

13. Audit Rights and Compliance Information

13.1. The Processor shall make available to the Congregation, on reasonable written request, information necessary to demonstrate compliance with this Agreement, to the extent required by applicable Data Protection Laws and to the extent such information is within the Processor's possession or control.

13.2. The Congregation's audit rights arise only to the extent that the Principal Agreement, Privacy Policy, this Agreement, available documentation, security information, subprocessor information, and other information provided by the Processor do not otherwise provide the Congregation with information and audit rights sufficient to meet applicable Data Protection Laws.

13.3. Any audit must be:

(a) requested on reasonable prior written notice;

(b) limited to the Processing of Congregation Personal Data by the Processor;

(c) conducted during normal business hours;

(d) conducted in a manner that does not unreasonably interfere with the Processor's business, security, confidentiality, systems, personnel, other customers, or Subprocessors;

(e) subject to reasonable confidentiality, security, and access restrictions;

(f) limited to information relevant to the Processor's compliance with this Agreement.

13.4. The Processor may satisfy an audit request by providing written responses, documentation, summaries, policies, certifications, third-party audit reports, security information, or other reasonable evidence of compliance.

13.5. The Processor is not required to disclose information that would compromise the security of the Services, disclose confidential information of other customers, expose trade secrets, disclose privileged information, violate law, or create an unreasonable security, operational, or confidentiality risk.

13.6. The Congregation shall bear its own costs of any audit unless applicable Data Protection Laws require otherwise.

14. Records and Cooperation

14.1. The Processor shall maintain records of categories of Processing activities carried out on behalf of the Congregation to the extent required by applicable Data Protection Laws.

14.2. The Processor shall cooperate with competent Supervisory Authorities to the extent required by applicable Data Protection Laws.

14.3. The Processor shall provide reasonable information to the Congregation to support the Congregation's own compliance obligations, taking into account the nature of the Processing, the information available to the Processor, and the Processor's inability to read Encrypted and Obfuscated Congregation Data.

15. Data Transfer

15.1. To the extent reasonably practicable, Congregation Data is stored and processed within the European Union or a country, territory, sector, or recipient recognized as providing an adequate level of protection under applicable Data Protection Laws.

15.2. Where the Services allow the Congregation to select a sharing server region, the Congregation may select the region used for Congregation Sharing. Encrypted and obfuscated data strings are stored in the selected sharing region unless changed by the Congregation, required for service operation, required by applicable law, or caused by the Congregation's own access location, configuration, device, Approved Users, or instructions.

15.3. For Congregations selecting an EU sharing region, the Processor uses Google Firebase and related Google Cloud infrastructure configured in Belgium.

15.4. The Processor does not transfer Congregation Data outside the European Union except for the following limited categories:

(a) the First Name and email address of Shared Persons, where such Processing is necessary to invite, identify, authenticate, notify, support, or provide access to the Services for such Shared Persons; and

(b) anonymous diagnostic data used for reliability, performance, security, fault detection, abuse prevention, service improvement, and operational diagnostics.

15.5. Encrypted and Obfuscated Congregation Data received from local NWS Desktop or NWS Mobile software is not transferred outside the European Union by the Processor for Congregations using the EU sharing region, except where the Congregation, its Approved Users, or the Congregation's own device, configuration, access location, or instructions cause such access, retrieval, download, synchronization, or transfer.

15.6. Anonymous diagnostic data is not intended to identify a natural person and is Processed only in a form that does not permit the Processor to identify a Data Subject. If diagnostic data is capable of identifying a natural person, it shall not be treated as anonymous diagnostic data under this Agreement.

15.7. Where any transfer of Personal Data outside the European Union, the European Economic Area, the United Kingdom, or an adequate jurisdiction is required, the Processor shall ensure that such transfer is made only in accordance with applicable Data Protection

Laws and, where required, is subject to an appropriate transfer mechanism, including the then-current EU Standard Contractual Clauses, UK International Data Transfer Agreement or Addendum, adequacy decision, derogation, Data Privacy Framework certification where applicable, or other lawful transfer mechanism.

15.8. If Standard Contractual Clauses or another mandatory transfer mechanism applies and conflicts with this Agreement, the applicable mandatory transfer mechanism shall prevail to the extent of the conflict.

16. Confidentiality

16.1. Each Party must keep confidential any non-public information it receives about the other Party, its business, systems, technology, users, data, security measures, pricing, operations, and records in connection with this Agreement ("Confidential Information").

16.2. A Party must not use or disclose Confidential Information except:

(a) to perform or receive the Services;

(b) to comply with this Agreement or the Principal Agreement;

(c) with the prior written consent of the other Party;

(d) where required by law;

(e) to professional advisers subject to confidentiality obligations;

(f) where the information is already in the public domain through no fault of the receiving Party.

16.3. Congregation Personal Data is Confidential Information of the Congregation.

16.4. The confidentiality obligations in this section survive termination of this Agreement.

17. Limitation of Liability

17.1. Each Party's liability under this Agreement is subject to the exclusions, limitations, caps, and other liability provisions in the Principal Agreement, unless prohibited by applicable law.

17.2. Nothing in this Agreement limits liability to the extent such limitation is prohibited by applicable law.

17.3. Nothing in this Agreement limits or excludes a Party's liability for fraud, wilful misconduct, or any other liability that cannot lawfully be limited or excluded.

18. Order of Precedence

18.1. If there is a conflict between this Agreement and the Principal Agreement in relation to the Processing of Congregation Personal Data by the Processor, this Agreement prevails to the extent of the conflict.

18.2. If there is a conflict between this Agreement and applicable Standard Contractual Clauses or another mandatory data transfer mechanism, the Standard Contractual Clauses or mandatory transfer mechanism prevail to the extent of the conflict.

18.3. If there is a conflict between this Agreement and the Privacy Policy in relation to the Processing of Congregation Personal Data by the Processor, this Agreement prevails to the extent of the conflict.

19. Notices

19.1. Notices and communications under this Agreement must be in writing and may be sent by email, through the Services, through account notices, through the Processor's website, or by another reasonable written method.

19.2. Notices to the Congregation may be sent to the email address associated with the Congregation's use of the Services.

19.3. Notices to the Processor may be sent to support@nwscheduler.com, or any other address notified by the Processor from time to time.

19.4. The Congregation is responsible for keeping its contact details current.

20. Governing Law and Jurisdiction

20.1. This Agreement is governed by the laws of New South Wales, Australia, without regard to conflict of law principles.

20.2. Subject to any mandatory rights or jurisdiction under applicable Data Protection Laws, the Parties submit to the exclusive jurisdiction of the courts of New South Wales, Australia for disputes arising out of or in connection with this Agreement, the Principal Agreement, New World Solutions technology, or the Services.

21. General Terms

21.1. The Processor will Process Congregation Personal Data in accordance with this Agreement and Data Protection Laws applicable to the Processor's role under this Agreement.

21.2. The Processor is not responsible for complying with Data Protection Laws that apply solely to the Congregation by virtue of the Congregation's activities, purposes, decisions, data entry, sharing decisions, religious status, membership records, lawful basis, notices, consents, internal governance, or relationship with Data Subjects.

21.3. The Congregation is responsible for determining whether its use of the Services complies with laws, policies, rules, governance requirements, and obligations applicable to the Congregation.

21.4. No failure or delay by either Party in exercising any right under this Agreement will constitute a waiver of that right.

21.5. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions remain in full force and effect.

21.6. This Agreement may be amended by the Processor from time to time where required to reflect changes in the Services, Data Protection Laws, Subprocessors, technical measures, or legal requirements. Where required by applicable law, the Processor will provide notice of material changes.

Schedule 1 — Details of Processing

1. Subject Matter of Processing

The subject matter of the Processing is the provision, operation, maintenance, support, security, synchronization, transfer, availability, and controlled distribution of Congregation Personal Data through the Services, including NWS Desktop, NWS Mobile, NW Publisher, and any related online, hosted, or synchronized services provided by the Processor.

The Processor receives data from the Congregation, or from persons approved by the Congregation, through local NWS Desktop or NWS Mobile software and makes such data available only to other approved users within the same Congregation, subject to the Congregation's configuration, permissions, approvals, and use of the Services.

2. Nature and Purpose of Processing

The Processor Processes Congregation Personal Data solely for the following purposes:

(a) receiving, storing, transmitting, synchronizing, and making available encrypted and obfuscated data strings received from the Congregation's local NWS Desktop or NWS Mobile software;

(b) making such encrypted and obfuscated data strings available to other approved users in the same Congregation, according to the permissions, approvals, configuration, and account settings determined by the Congregation;

(c) providing authentication, account access, support, service availability, synchronization, security, abuse prevention, diagnostic, and operational functions necessary for the Services;

(d) maintaining service integrity, preventing unauthorized access, detecting service errors, resolving technical issues, and complying with applicable legal obligations;

(e) processing the First Name and email address of Shared Persons where necessary to identify, invite, authenticate, notify, or make available the Services to such Shared Persons; and

(f) processing anonymous diagnostic data for operational, reliability, performance, security, and error-detection purposes.

3. Categories of Data Subjects

The Processor does not know, determine, inspect, or verify the categories of Data Subjects whose Personal Data may be contained within Encrypted and Obfuscated Congregation Data.

The categories of Data Subjects are determined solely by the Congregation and may include any individuals whose Personal Data the Congregation chooses to enter, store, synchronize, share, or otherwise process through local NWS Desktop or NWS Mobile software.

For data that is not contained within Encrypted and Obfuscated Congregation Data, the categories of Data Subjects are limited to Approved Users and Shared Persons whose First Name and email address are processed for account invitation, access, authentication, identification, notification, support, or service availability.

4. Categories of Personal Data

The Processor does not know, determine, inspect, access, read, or verify the categories of Personal Data contained within Encrypted and Obfuscated Congregation Data.

For Encrypted and Obfuscated Congregation Data, the type of Personal Data processed by the Processor is limited to encrypted and obfuscated data strings received from local NWS Desktop or NWS Mobile software, together with technical metadata necessary to receive, store, transmit, synchronize, make available, and delete those strings.

The plaintext contents of Encrypted and Obfuscated Congregation Data are determined solely by the Congregation and are not accessible to the Processor.

For data that is not contained within Encrypted and Obfuscated Congregation Data, the categories of Personal Data processed by the Processor are limited to:

(a) the First Name and email address of Shared Persons;

(b) account identifiers, access identifiers, authentication metadata, configuration values, timestamps, synchronization metadata, service metadata, and operational records necessary to provide, secure, maintain, support, and troubleshoot the Services; and

(c) anonymous diagnostic data, provided that diagnostic data capable of identifying a natural person is not treated as anonymous diagnostic data under this Agreement.

5. Encrypted and Obfuscated Congregation Data

Except for the limited categories expressly identified in this Schedule, the Processor stores Congregation Personal Data received from local NWS Desktop or NWS Mobile software only as encrypted and obfuscated strings.

Such encrypted and obfuscated strings are protected using end-to-end encryption. The Processor does not possess, store, derive, recover, or otherwise have access to the decryption keys required to read the contents of those encrypted and obfuscated strings. Accordingly, the Processor cannot read, inspect, interpret, search, access, disclose, or use the plaintext contents of such encrypted and obfuscated strings, including by its employees, contractors, support personnel, administrators, infrastructure providers, or other representatives.

The Processor's role in respect of such encrypted and obfuscated strings is limited to receiving, storing, transmitting, synchronizing, and making available those strings to approved users in the Congregation in accordance with the Congregation's instructions and permissions.

6. Special Categories of Data

The Services are not intended for the submission of special categories of personal data unless the Congregation determines that such Processing is necessary and lawful. The Congregation is responsible for determining the lawful basis, necessity, proportionality, and accuracy of any Personal Data submitted to the Services, including any data that may constitute special category data under applicable Data Protection Laws.

7. Duration of Processing

The Processor will Process Congregation Personal Data for the duration of the Principal Agreement and for such further period as is necessary to provide the Services, comply with applicable legal obligations, resolve disputes, maintain security, or complete deletion in accordance with this Agreement.

Inactive data is automatically deleted after 60 days, unless a longer retention period is required by applicable law, necessary to complete a user-requested operation, or otherwise expressly agreed with the Congregation.

8. Controller Rights and Obligations

The Congregation determines the purposes and means of Processing Congregation Personal Data. The Congregation is responsible for ensuring that it has a lawful basis for collecting, entering, uploading, synchronizing, sharing, and otherwise Processing Congregation Personal Data through the Services.

The Congregation is responsible for ensuring that approved users are authorized to access the data made available to them and that account permissions, sharing permissions, and user approvals are accurate and kept up to date.

The Congregation may instruct the Processor to delete Congregation Personal Data through the functionality made available in the Services or by making a written request to the Processor.

Schedule 2 — Technical and Organisational Measures

1. Optional Congregation Sharing

Congregation Sharing is optional and is enabled, configured, and controlled by the Congregation. The Congregation determines whether Congregation Sharing is enabled, which persons are approved to access shared data, which permissions apply, and which sharing server region is selected where such selection is made available by the Services.

2. Encryption and Obfuscation

The Processor stores Congregation Data received from local NWS Desktop or NWS Mobile software as encrypted and obfuscated strings, except for limited Personal Data expressly identified in this Agreement.

Encrypted and Obfuscated Congregation Data is encrypted on the local device before transfer. Encryption keys are generated locally and are not transferred to, stored by, or made available to the Processor or the sharing server. The Processor does not possess, store, derive, recover, or otherwise have access to the keys necessary to read the plaintext contents of that data.

The Services use end-to-end symmetric encryption for Encrypted and Obfuscated Congregation Data. The encryption key length is 256-bit. Keys are derived locally using password-based key derivation, including Argon2id and SHA-256. A random and unique initialization vector and salt are generated for each item of transferred data where applicable.

3. Authentication and Authorization

Where Congregation Sharing is used, access is protected by authentication and authorization controls, which may include OAuth 2.0 authorization, access tokens, refresh tokens, Congregation ID, Congregation Sharing Password, email identification, device verification, and verification codes.

Congregation Sharing Passwords are not stored by the Processor and are not stored on the sharing server. The Congregation is responsible for selecting, distributing, rotating, and protecting Congregation Sharing Passwords.

Where password controls are enforced by the Services, the Services require strong passwords of at least 12 characters, including lowercase letters, uppercase letters, numbers, and symbols.

4. Access Control

The Processor maintains access controls intended to restrict access to systems used to provide the Services to persons who require such access for legitimate operational, support, security, legal, or administrative purposes.

Approved User access is controlled by the Congregation's configuration, permissions, approvals, and account settings.

Access credentials are scoped to the relevant Congregation. Approved Users are not authorized to access encrypted and obfuscated data strings belonging to any other congregation.

5. Unique and Obfuscated Storage Location

Each Congregation is assigned a unique and obfuscated storage location for encrypted and obfuscated data strings. Access to that location is restricted to Approved Users who satisfy the applicable authentication and authorization requirements.

6. Logical Separation

The Processor uses logical separation measures intended to prevent Congregation Data from being made available to unauthorized congregations or unauthorized users.

7. Transport Security

Data in transit is transmitted using encrypted transport security, including TLS 1.2 or higher where supported. TLS 1.0 and TLS 1.1 are not used for Congregation Sharing data transfer.

8. Server Region Selection

The Congregation may select the sharing server region used for Congregation Sharing where such selection is made available by the Services. Encrypted and obfuscated data strings are stored in the selected sharing region unless changed by the Congregation, required for service operation, required by applicable law, or caused by the Congregation's own access location, configuration, device, Approved Users, or instructions.

9. Google Firebase Infrastructure

The Processor uses Google Firebase and related Google Cloud Platform services as its only appointed infrastructure Subprocessor for hosted storage, authentication, serverless processing, synchronization, encrypted data transfer, service security, diagnostics, and related technical infrastructure required for the Services.

Google's published Firebase and Google Cloud security information describes technical and organisational measures including physically secure data centres, redundancy, business continuity planning, internal access controls, personnel confidentiality obligations, incident response procedures, encryption technologies, HTTPS/TLS availability, and subprocessor security controls.

Google states that Firebase services have completed ISO 27001 and SOC 1, SOC 2, and SOC 3 evaluation processes, and that some Firebase services have also completed ISO 27017 and ISO 27018 certification processes. Google Cloud Platform is also certified as ISO/IEC 27001:2022 compliant and ISO/IEC 27018 compliant.

10. Availability and Integrity

The Processor uses reasonable operational measures intended to maintain service availability, detect errors, preserve service integrity, and support secure synchronization of encrypted and obfuscated data strings.

Google Firebase and related Google Cloud infrastructure may use redundancy, replication, and other technical measures to protect service availability, integrity, and resilience. Such technical infrastructure measures do not give the Processor access to the plaintext contents of Encrypted and Obfuscated Congregation Data and are not maintained by the Processor as separate backup copies of Congregation Data.

11. Deletion

The Processor provides deletion functionality where available in the Services and automatically deletes inactive data after 60 days, subject to the exceptions stated in this Agreement.

If the Congregation disables Congregation Sharing, the encrypted and obfuscated data strings stored for Congregation Sharing are deleted from the sharing server through the normal operation of the Services.

The Processor does not create backup copies of Congregation Data or maintain separate retained copies of deleted Congregation Data, except where transient technical replication, infrastructure redundancy, or temporary operational processing is strictly necessary for immediate service operation and is not retained by the Processor as a separate backup copy.

12. Diagnostics

The Processor may process anonymous diagnostic data for service reliability, performance, security, error detection, abuse prevention, and operational diagnostics.

Diagnostic data that is capable of identifying a natural person is not treated as anonymous diagnostic data under this Agreement.

13. Subprocessor Controls

The Processor requires any directly appointed Subprocessor to protect Congregation Data using written obligations no less protective than this Agreement, to the extent applicable to the services provided by the Subprocessor.

14. Security Review

The Processor reviews and improves technical and organisational measures where reasonably appropriate, having regard to the nature, scope, context, purpose, and risk of Processing.

Schedule 3 — Restricted Data Transfer Terms

1. Restricted Transfers

Where Congregation Personal Data is transferred outside the European Union, European Economic Area, United Kingdom, or an adequate jurisdiction, and such transfer is subject to transfer restrictions under applicable Data Protection Laws, the Processor shall ensure that an appropriate lawful transfer mechanism is used.

2. Standard Contractual Clauses

Where required, the Parties shall rely on the then-current EU Standard Contractual Clauses, UK International Data Transfer Agreement, UK Addendum, adequacy decision, derogation, or other valid transfer mechanism.

3. Limited Exceptions

The Processor does not transfer Congregation Personal Data outside the European Union except for the First Name and email address of Shared Persons and anonymous diagnostic data, as described in this Agreement.

4. Encrypted Data

Encrypted and Obfuscated Congregation Data is not transferred outside the European Union by the Processor except where such transfer is caused by the Congregation, an Approved User, or the Congregation’s own access location, configuration, device, or instruction.