DATA PROCESSING AGREEMENT

THIS AGREEMENT IS BETWEEN:

1) The Parish/Town Council ("Data Controller")

2) Northamptonshire County Association of Local Councils Limited a company registered in England under number 7335699 ("Data Processor")

WHEREAS:

1) The Data Controller from time to time engages the Data Processor to provide to the Data Controller the Services described in Schedule 1.

2) The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

3) Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR") requires an agreement in writing between the Data Controller and any organisation which processes Personal Data on its behalf, governing the processing of that Personal Data.

4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the UK GDPR in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1. In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller"	shall have the meaning given to the term "controller" in section 6 of the Data Protection Act 2018;
"Data Processor"	shall have the meaning given to the term "processor" in Article 4 of the UK GDPR;
"Data Protection Legislation"	means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended;

“Data Subject”	shall have the meaning given to the term “data subject” in Article 4 of the UK GDPR
“EEA”	means the European Economic Area, consisting of all EU Member States plus Iceland, Liechtenstein, and Norway
“Information Commissioner”	means the Information Commissioner, as defined in Article 4(A3) of the UK GDPR and section 114 of the Data Protection Act 2018
“Personal Data Breach”	shall have the meaning given to the term “personal data breach” in Article 4 of the UK GDPR
“Personal Data”	means all such “personal data”, as defined in Article 4 of the UK GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2
“processing”, “process”, “processes”, “processed”	shall have the meaning given to the term “processing” in Article 4 of the UK GDPR
“Services”	means those services described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose[s] described in Schedule 1
“Standard Contractual Clauses”	means the European Commission’s Standard Contractual Clauses for the transfer of Personal Data from the European Union to data processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU (incorporating UK-centric contextual amendments made by the Information Commissioner)
“Term”	means the term of this Agreement, as set out in Clause 17

1.2. Unless the context otherwise requires, each reference in this Agreement to:

1.2.a. “writing”, and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

1.2.b. a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.c. “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

1.2.d. a Schedule is a schedule to this Agreement;

1.2.e. a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule; and

1.2.f. a "Party" or the "Parties" refer to the parties to this Agreement.

1.3. The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4. Words imparting the singular number shall include the plural and vice versa.

1.5. References to any gender shall include any other gender.

1.6. References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1. The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Data Controller by the Data Processor, and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

2.2. In the event of any conflict or ambiguity between any of the provisions of this Agreement and any other agreement between the Parties, the provisions of this Agreement shall prevail.

2.3. In the event of any conflict or ambiguity between any of the provisions of this Agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

3. Provision of the Services and Processing Personal Data

3.1. Schedule 2 describes the type(s) of Personal Data, the category or categories of Data Subject, the nature of the processing to be carried out, the purpose(s) of the processing, and the duration of the processing.

3.2. Subject to sub-Clause 4.1, the Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

3.2.a. for the purposes of those Services and not for any other purpose;

3.2.b. to the extent and in such a manner as is necessary for those purposes; and

3.2.c. strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

3.3. The Data Controller shall retain control of the Personal Data at all times and shall remain responsible for its compliance with the relevant Data Protection Legislation including, but not limited to, its collection, holding, and processing of the Personal Data, having in place all necessary and appropriate consents and notices to enable the lawful transfer of the Personal Data to the Data Processor, and with respect to the written instructions given to the Data Processor.

4. The Data Processor's Obligations

4.1. As set out above in Clause 3, the Data Processor shall only process the Personal Data to the extent and in such a manner as is necessary for the purposes of the Services and not for any other purpose. All instructions given by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the Data Protection Legislation. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by domestic law to do otherwise (as per Article 29 of the UK GDPR) (in

which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law).

4.2. The Data Processor shall not process the Personal Data in any manner which does not comply with the provisions of this Agreement or with the Data Protection Legislation.

4.3. The Data Processor shall promptly comply with any written request from the Data Controller requiring the Data Processor to amend, transfer, delete (or otherwise dispose of), or to otherwise process the Personal Data.

4.4. The Data Processor shall promptly comply with any written request from the Data Controller requiring the Data Processor to stop, mitigate, or remedy any unauthorised processing involving the Personal Data.

4.5. The Data Processor shall provide all reasonable assistance at the Data Controller's cost to the Data Controller in complying with its obligations under the Data Protection Legislation including, but not limited to, the protection of Data Subjects' rights, the security of processing, the notification of Personal Data Breaches, the conduct of data protection impact assessments, and in dealings with the Information Commissioner (including, but not limited to, consultations with the Information Commissioner where a data protection impact assessment indicates that there is a high risk which cannot be mitigated).

4.6. For the purposes of sub-Clause 4.5, "all reasonable assistance" shall take account of the nature of the processing carried out by the Data Processor and the information available to the Data Processor.

4.7. In the event that the Data Processor becomes aware of any changes to the Data Protection Legislation that may, in its reasonable interpretation, adversely impact its performance of the Services and the processing of the Personal Data under this Agreement, the Data Processor shall inform the Data Controller promptly.

5. Confidentiality

5.1. The Data Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose the Personal Data to any third party. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than as necessary and for the purposes of the provision of the Services to the Data Controller.

5.2. Nothing in this Agreement shall prevent the Data Processor from complying with any requirement to disclose or process Personal Data where such disclosure or processing is required by domestic law, court, or regulator (including, but not limited to, the Information Commissioner). In such cases, the Data Processor shall notify the Data Controller of the disclosure or processing requirements prior to disclosure or processing (unless such notification is prohibited by domestic law) in order that the Data Controller may challenge the requirement if it wishes to do so.

5.3. The Data Processor shall ensure that all employees who are to access and/or process any of the Personal Data are informed of its confidential nature and are contractually obliged to keep the Personal Data confidential.

6. Employees

6.1. The Data Processor shall ensure that all employees who are to access and/or process any of the Personal Data are given suitable training on the Data Protection Legislation, the Data Processor's obligations under it, their obligations under it, and its application to their work, with particular regard to the processing of the Personal Data under this Agreement.

7. Security of Processing

7.1. The Data Processor shall implement appropriate technical and organisational measures as described in Schedule 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage. The Data Processor shall inform the Data Controller in advance of any changes to such measures.

7.2. The measures implemented by the Data Processor shall be appropriate to the nature of the personal data, to the harm that may result from such unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage (in particular to the rights and freedoms of Data Subjects) and shall have regard for the state of technological development and the costs of implementation.

7.3. The measures implemented by the Data Processor may include, as appropriate, pseudonymisation and encryption of the Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures.

8. Data Subject Rights and Complaints

8.1. The Data Processor shall take appropriate technical and organisational measures and provide all reasonable assistance at the Data Controller's cost to the Data Controller in complying with its obligations under the Data Protection Legislation with particular regard to the following:

8.1.a. the rights of Data Subjects under the Data Protection Legislation including, but not limited to, the right of access (data subject access requests), the right to rectification, the right to erasure, portability rights, the right to object to processing, rights relating to automated processing, and rights to restrict processing; and

8.1.b. compliance with notices served on the Data Controller by the Information Commissioner pursuant to the Data Protection Legislation.

8.2. In the event that the Data Processor receives any notice, complaint, or other communication relating to the Personal Data processing or to either Party's compliance with the Data Protection Legislation, it shall notify the Data Controller immediately in writing.

8.3. In the event that the Data Processor receives any request from a Data Subject to exercise any of their rights under the Data Protection Legislation including, but not limited to, a data subject access request, it shall notify the Data Controller without undue delay.

8.4. The Data Processor shall cooperate fully at the Data Controller's cost with the Data Controller and provide all reasonable assistance in responding to any complaint, notice, other communication, or Data Subject request, including by:

8.4.a. providing the Data Controller with full details of the complaint or request;

8.4.b. providing the necessary information and assistance in order to comply with a subject access request;

8.4.c. providing the Data Controller with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Data Controller); and

8.4.d. providing the Data Controller with any other information requested by the Data Controller.

8.5. The Data Processor shall act only on the Data Controller's instructions and shall not disclose any Personal Data to any Data Subject or to any other party except as instructed in writing by the Data Controller, or as required by domestic law.

9. Personal Data Breaches

9.1. The Data Processor shall within 36 (hours) (and without undue delay) notify the Data Controller in writing if it becomes aware of any form of Personal Data Breach including, but not limited to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data.

9.2. When the Data Processor becomes aware of a Personal Data Breach, it shall provide the following information to the Data Controller in writing without undue delay:

9.2.a. a description of the Personal Data Breach including the category or categories of Personal Data involved, the number (approximate or exact, if known) of Personal Data records involved, and the number (approximate or exact, if known) of Data Subjects involved;

9.2.b. the likely consequences of the Personal Data Breach; and

9.2.c. a description of the measures it has taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3. In the event of a Personal Data Breach as described above, the Parties shall cooperate with one another to investigate it. The Data Processor shall provide all reasonable assistance to the Data Controller including, but not limited to:

9.3.a. assisting the Data Controller with its investigation of the Personal Data Breach;

9.3.b. providing and facilitating the Data Controller with access to any relevant facilities, operations, and personnel (including, if applicable, former personnel involved in the Personal Data Breach);

9.3.c. making available all records, logs, files, reports, and similar as reasonably required by the Data Controller or as otherwise required by the Data Protection Legislation; and

9.3.d. promptly taking all reasonable steps to mitigate the effects of the Personal Data Breach and to minimise any damage caused by it.

9.4. The Data Processor shall use all reasonable endeavours to restore any Personal Data lost, destroyed, damaged, corrupted, or otherwise rendered unusable in the Personal Data Breach as soon as possible after becoming aware of the Personal Data Breach.

9.5. The Data Processor shall not inform any third party of any Personal Data Breach as described above without the express written consent of the Data Controller unless it is required to do so by domestic law.

9.6. The Data Controller shall have the sole right to determine whether or not to notify affected Data Subjects, the Information Commissioner, law enforcement agencies, or other applicable

regulators of the Personal Data Breach as required by law or other applicable regulations, or at the Data Controller's discretion, including the form of such notification.

9.7. The Data Controller shall have the sole right to determine whether or not to offer any remedy to Data Subjects affected by the Personal Data Breach, including the form and amount of such remedy.

9.8. Subject to the provisions of Clause 16, the Data Processor shall bear all reasonable costs and expenses incurred by it and shall reimburse the Data Controller for all reasonable costs and expenses incurred by the Data Controller in responding to the Personal Data Breach, including the exercise of any functions or carrying out of any obligations by the Data Controller under any provision of this Clause 9, unless the Personal Data Breach resulted from the Data Controller's express written instructions, negligence, breach of this Agreement, or other act or omission of the Data controller, in which case the Data Controller shall instead bear and shall reimburse the Data Processor with such costs and expenses incurred by it.

10. Cross-Border Transfers of Personal Data

10.1. The Data Processor and any subcontractor appointed by it) may process or transfer the Personal Data outside of the EEA without the prior written consent of the Data Controller.

10.2. The Data Processor may only process (or permit the processing) of the Personal Data outside of the EEA if one or more of the following conditions are satisfied:

10.2.a. the Data Processor is processing the Personal Data in a territory that is subject to adequacy regulations under the Data Protection Legislation that said territory provides adequate protection for the privacy rights of individuals. The territories subject to such a finding shall be identified in Schedule 4;

10.2.b. the Data Processor participates in a valid cross-border transfer mechanism under the Data Protection Legislation under which the Data Processor (and the Data Controller, where appropriate) can ensure that appropriate safeguards are in place to ensure an adequate level of data protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR. The transfer mechanism enabling such transfers is identified in Schedule 4; or

10.2.c. the transfer of the Personal Data otherwise complies with the Data Protection Legislation for the reasons set out in Schedule 4.

10.3. In the event that the Data Processor appoints a subcontractor, in accordance with the provisions of Clause 11, and the subcontractor is located outside of the EEA, the Data Controller hereby authorises the Data Processor to enter into Standard Contractual Clauses, with the subcontractor. The Data Processor shall make said executed Standard Contractual Clauses available to the Data Controller on request.

11. Appointment of Subcontractors

11.1. In the event that the Data Processor appoints a subcontractor to process any of the Personal Data, the Data Processor shall:

11.1.a. enter into a written agreement with each subcontractor, which shall impose upon the subcontractor the same obligations, on substantially the same terms, as are imposed upon the Data Processor by this Agreement, particularly with regard to technical and organisational security measures required to comply with the Data Protection Legislation, which shall permit both the Data Processor and the Data Controller to

enforce those obligations, and which shall terminate automatically on the termination of this Agreement for any reason;

11.1.b. at the written request of the Data Controller, provide copies of such agreements or, as applicable, the relevant parts thereof;

11.1.c. ensure that all subcontractors comply fully with their obligations under the abovementioned agreement and under the Data Protection Legislation; and

11.1.d. maintain control over all Personal Data transferred to subcontractors.

12. Return and/or Deletion or Disposal of Personal Data

12.1. The Data Processor shall, at the written request of the Data Controller (and at the Data Controller's choice), securely delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

12.1.a. the end of the provision of the Services; or

12.1.b. the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor's obligations under this Agreement.

12.2. Subject to sub-Clause 12.3, the Data Processor shall not retain all or any part of the Personal Data after deleting (or otherwise disposing of) or returning it under sub-Clause 12.1.

12.3. If the Data Processor is required to retain copies of all or any part of the Personal Data by law, regulation, government, or other regulatory body, it shall inform the Data Controller of such requirement(s) in writing, including precise details of the Personal Data that it is required to retain, the legal basis for the retention, details of the duration of the retention, and when the retained Personal Data will be deleted (or otherwise disposed of) once it is no longer required to retain it.

13. Information

13.1. The Data Processor shall make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor's compliance with the Data Protection Legislation and this Agreement.

14. Audits

14.1. The Data Processor shall, on reasonable prior notice, allow the Data Controller or a third-party auditor appointed by the Data Controller to audit the Data Processor's compliance with its obligations under this Agreement and with the Data Protection Legislation.

14.2. The Data Processor shall provide all necessary assistance (at the Data Controller's cost) in the conduct of such audits including, but not limited to:

14.2.a. access (including physical and remote) to, and copies of, all relevant information kept by the Data Processor;

14.2.b. access to all of its employees who are to access and/or process any of the Personal Data including, where reasonably necessary, arranging interviews between the Data Controller and such employees; and

14.2.c. access to and the inspection of all infrastructure, equipment, software, and other systems used to store and/or process the Personal Data.

14.3. The Data Processor must inform the Data Controller promptly if, in its opinion, any instructions given by the Data Controller or any third-party auditor appointed by the Data Controller do not comply with the Data Protection Legislation.

15. Warranties

15.1. The Data Controller hereby warrants and represents that the Personal Data and its use with respect to the Services and this Agreement shall comply with the Data Protection Legislation in all respects including, but not limited to, its collection, holding, and processing.

15.2. The Data Processor hereby warrants and represents that:

15.2.a. the Personal Data shall be processed by the Data Processor (and by any subcontractors appointed under Clause 11) in compliance with the Data Protection Legislation and any and all other relevant laws, regulations, enactments, orders, standards, and other similar instruments;

15.2.b. it has no reason to believe that the Data Protection Legislation in any way prevents it from complying with its obligations pertaining to the provision of the Services; and

15.2.c. it will implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage, as set out in Clause 7 and described in Schedule 3.

16. Liability and Indemnity

16.1. The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of, any and all actions, proceedings, liabilities, costs, claims, losses, expenses (including reasonable legal fees and payments on a solicitor and client basis), or demands, suffered or incurred by, awarded against, or agreed to be paid by, the Data Processor and any subcontractor appointed by the Data Processor under Clause 11 arising directly or in connection with:

16.1.a. any non-compliance by the Data Controller with the Data Protection Legislation;

16.1.b. any Personal Data processing carried out by the Data Processor or any subcontractor appointed by the Data Processor under Clause 11 in accordance with instructions given by the Data Controller to the extent that the instructions infringe the Data Protection Legislation; or

16.1.c. any breach by the Data Controller of its obligations or warranties under this Agreement;

but not to the extent that the same is or are contributed to by any non-compliance by the Data Processor or any subcontractor appointed by the Data Processor under Clause 11 with the Data Protection Legislation or its breach of this Agreement.

16.2. The Data Controller shall not be entitled to claim back from the Data Processor under sub-Clause 16.2 or on any other basis any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Processor under sub-Clause 16.1.

16.3. Nothing in this Agreement (and in particular, this Clause 16) shall relieve either Party of, or otherwise affect, the liability of either Party to any Data Subject, or for any other breach of that Party's direct obligations under the Data Protection Legislation. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the Information Commissioner and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in the Data Protection Legislation.

16.4. Subject to sub-Clause 2.4, nothing in this Clause 16 shall be deemed to be limited, excluded, or prejudiced by any other provision(s) of this Agreement.

17. Term and Termination

17.1. This Agreement shall come into force when agreed to and shall continue in force for the longer of:

17.1.a. The duration of the Services, as set out in Schedule 1; or

17.2. Any provision of this Agreement which, expressly or by implication, is to come into force or remain in force on or after its termination or expiry shall remain in full force and effect.

17.3. In the event that changes to the Data Protection Legislation necessitate the re-negotiation of any part of this Agreement, either Party may require such re-negotiation.

18. Notices

18.1. All notices under or in connection with this Agreement shall be in writing.

18.2. All notices given to the Data Controller under or in connection with this Agreement must be addressed to the Data Controller at their listed address.

18.3. All notices given to the Data Processor under or in connection with this Agreement must be addressed to: Darren Briddock, Data protection officer, Breakthrough Communications & Strategies Limited, Mocatta House, Trafalgar Place, Brighton, England, BN1 4DU.

18.4. Notices shall be deemed to have been duly given:

18.4.a. when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours of the recipient; or

18.4.b. when sent, if transmitted by e-mail and a return receipt is generated; or

18.4.c. on the fifth business day following mailing, if mailed by national ordinary mail, postage prepaid.

In each case notices shall be addressed as indicated above.

19. Law and Jurisdiction

19.1. This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

19.2. Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

20. Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 7:

20.1. The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:

20.2. the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and

20.3. the nature of the Personal Data.

In particular, the Data Processor shall:

20.4. have in place, and comply with, data protection processes which:

20.4.a. defines security needs based on a risk assessment;

20.4.b. allocates responsibility for implementing the policy to a specific individual (such as the Data Processor's data protection officer) or personnel;

20.5. ensure that appropriate security safeguards are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

20.6. ensure that all hardware and software used in the processing of the Personal Data is properly maintained, including but not limited to, the installation of all applicable software updates;

20.7. prevent unauthorised access to the Personal Data;

20.8. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

20.9. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption);

20.10. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;

20.11. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

20.12. ensure that all employees who are to access and/or process any of the Personal Data are given suitable training on the Data Protection Legislation, the Data Processor's obligations under it, their obligations under it, and its application to their work, with particular regard to the processing of the Personal Data under this Agreement;

20.13. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

20.13.a. the ability to identify which individuals have worked with specific Personal Data;

20.13.b. having a proper procedure in place for investigating and remedying breaches of the Data Protection Legislation; and

20.13.c. notifying the Data Controller as soon as any such security breach occurs.

21. Legal Basis for Processing Personal Data Outside the EEA

The Data Processor's legal basis for processing the Personal Data outside of the EEA in order to comply with cross-border transfer restrictions is as follows:

Standard Contractual Clauses between the Data Processor as the "data exporter" on behalf of the Data Controller and the Data Processor's affiliate or subcontractor as the "data importer".

Schedule 1

We offer face to face, telephone and e-mail support to all member councils through:

- The Member Enquiry Service (MES) for straightforward, generic queries.
- Free at the point of use advisory service for complex or council-specific enquiries.
- "Quick Response" Legal Service, delivered through our partners, Wellers Hedley Solicitors.
- Human Resources advice, from recruitment through personnel management to handling the end of the employment relationship.
- Financial advice, including audit, governance, and accountability.
- Funding advice, including how to access external grant funding and administration of borrowing approval applications.
- Access to the Legal Team at the National Association of Local Councils (NALC).

Membership allows access to events, briefings, and seminars at member rates (doubled for non-members or those from outside Northamptonshire):

- Basic training courses for clerks and councillors.
- Advanced training for those wanting to push their skills or develop specialist knowledge.
- The Councillor Development Framework (CDF) to guide councillors on their learning journey.
- The Officer Development Framework (CDF) to guide clerks and other senior council officers on their learning journey.
- Formal qualifications, including the Certificate in Local Council Administration (CiLCA).
- Bespoke in-house training sessions so that the whole council learns together.
- One-off briefings and seminars on topics of particular interest.

. The information service includes:

- A weekly e-mail bulletin on topical issues (the Friday mini *eUpdate*).
- Timely e-mail alerts on significant developments.
- The bi-monthly *eUpdate*, containing timely and relevant features and articles.
- The Association's web site, with a county-wide directory of councils and council services.
- Access to NALC bulletins, Legal Topic Notes and Legal Briefings.

We maintain relationships with local government and community organisations in the county as well as building links at regional, national, and even international level by:

- Regular meetings with unitary council officers and elected members.
- Representing parish and town councils on boards and panels whose work impacts on our member councils (e.g. Superfast Northamptonshire Board).
- Electing directors as representatives to various outside bodies.
- Responding to local, regional and national consultations that affect member councils.
- Gathering member councils' views through surveys, seminars, and conferences.
- Consulting the Northants CALC Councillor Panel, giving a direct voice to parish and town councillors and ensuring that the diverse nature of member councils is represented.

- Understanding and responding to the issues that affect larger councils through the Northamptonshire Larger Councils Partnership (NLCP), a grouping of the thirty largest parish and town councils in the county.
- Representing parish and town councils in Northamptonshire at the Federation of East Midlands Associations of Local Councils (FEMALC).
- Lobbying the National Association of Local Councils (NALC) for policy and legislative changes to benefit member councils.

All councils must appoint an internal auditor who is independent and competent. Since 2000 Northants CALC has managed a panel of auditors on behalf of member councils that:

- Provides independent auditors, most of whom are practitioners in the county.
- Offers affordable rates for internal audit (doubled for non-member councils).
- Ensures auditors are competent through quarterly briefing meetings.
- Supports councils to improve governance and accountability standards and avoid expensive fines and penalties.

Northants CALC manages and administers the PLR Scheme where every parish and town council and parish meeting appoints a person (who could be a councillor, officer, or member of the public) to act as a single point of contact for the police. It is the same principle as the Parish Paths Warden Scheme for rights of way and the Highways Representative Scheme for highways

Schedule 2

COLUMN A	COLUMN B	COLUMN C	COLUMN D	COLUMN E	COLUMN F	COLUMN G	COLUMN H	COLUMN I
Information type	**What personal information (data) is collected?**	**Category of individual**	**Where does the data go?**	**Where and how is the data stored?**	**What security measures do you use?**	**Why do you need the data? Processing purpose**	**Lawful basis for processing**	**How long do you retain the data?**
Information in								
Email in	Email address, persons name, phone number,home or business address	Councillor/clerk/employee/contractor/board member/CALC officer/supplier/potential supplier/MP/member of the public	To the intended recipient/board meeting	Email server/hard drive/hard copy	Password/encryption	Management	Public interest/legal obligation/contract	As long as necessary
Phone message	Persons name, phone number	Councillor/clerk/employee/contractor/board member/CALC officer/supplier/potential supplier/MP/member of the public	To the intended recipient	Telephone system/written note/email	None	Management	Public interest/contract/legal obligation	Until actioned
Phone call	Persons name, phone number and possibily email address for follow up	Councillor/clerk/employee/contractor/board member/CALC officer/supplier/potential supplier/MP/member of the public	To recipient	Notebook/email system	None	Management	Public interest/legal obligation/contract	Until actioned
Invoices	Persons name, email address, address, bank details	Contractor/meeting venue/catering/NALC	To recipient	Filing cabinet/email system/hard drive/memory stick/removal hard drive	Password/encryption	Sales	Contract/legal obligation/public interest	last completed audit year
Newsletters	Email address, persons name and possibly phone number	Resident/contractor/NALC	To recipient	Filing cabinet/email system/hard drive	Password/encryption	Management	Contract/public interest	As long as necessary

Letters	Persons name, address, email address, telephone number	Councillor/clerk/employee/contractor/board member/CALC officer	To the intended recipient/board meeting	Filing cabinet/hard drive/email server	Password/encryption	Management	Legal obligation/public interest	As long as necessary
Photographs	Name, address	Councillor/clerk/employee/contractor/board member/CALC officer	Website/newsletter/archive	Hard drive/cloud/filing cabinet	Password/encryption	Management	Consent	As long as necessary
Lease agreements	Name, address, telephone number	Solicitor/land owner	To the intended recipient/board meeting/solicitor/NALC	Hard drive/cloud/filing cabinet	Password/encryption	Management	Contract	12 years
Contractors insurance documents	Name, address, telephone number	Contractor	To the intended recipient	Hard drive/cloud/filing cabinet	Password/encryption	Legal requirement	Contract	6 years
Grant applications	Name, address, telephone number, email, bank details	Clerk	To the intended recipient	Hard drive/cloud/filing cabinet	Password/encryption	Management/Financial	Public interest	3 years
Loan applications	Name, address, telephone number, email, bank details	Clerk	To the intended recipient/DLUHC	Hard drive/cloud/filing cabinet	Password/encryption	Management	Legal obligation	6 years
Consent forms	Name, address, telephone number, email	Councillor/clerk/employee/contractor/board member/CALC officer	To the intended recipient	Hard drive/cloud/filing cabinet	Password/encryption	Management	Consent	6 years
Record of consents	Name, address, telephone number, email	Councillor/clerk/employee/contractor/board member/CALC officer	To the intended recipient	Hard drive/cloud/filing cabinet	Password/encryption	Management	Consent/legal obligation	6 years
Accident book	Name, address, telephone number, email	Employee/visitor	To the intended recipient, HSE	Filing cabinet	Locked office	Legal requirement	Legal obligation	3 years
Training requests	Name, email, phone number	Clerk/councillor	To the intended recipient	Hard drive/cloud/filing cabinet/email	Password/encryption	Management	Legal obligation	3 years
Membership	Name, address, telephone number, email	Clerk/Chairman	To the intended recipient	Hard drive/email	Password/encryption	Management	Contract	6 years
Survey results	Name, email address, council	Board, councillor panel	To the intended recipient, Update article	Hard drive/cloud/filing cabinet/email	Password/encryption	Management	Consent	3 years

Council FOI/SAR requests	Name, address, telephone number, email of clerk and name/email of third party raising the request to the council	Councillor/clerk/employee/member of the public	To the intended recipient	Email/hard drive/cloud	Password/encryption	Management	Public interest/legal obligation/contract	As long as necessary
Information out								
Email out	Email address, persons name	Councillor/clerk/employee/contractor/board member/CALC officer	To intended recipients	Email	Password/encryption	Management	Contract/legal obligation/consent	As long as necessary
Invoices sent hard copy	Name, address, bank details	Clerk	To intended recipients	Hard drive/filing cabinet/cloud	Password/encryption	Management	Contract	Last completed audit year
Invoices sent via email	Email address, persons name, bank details	Clerk	To intended recipients	Email/hard drive/filing cabinet/cloud	Password/encryption	Management	Contract	7 years
Newsletters	Email address, persons name, address, photos	Clerk	To intended recipients/website	Email/hard drive/cloud	Password/encryption	Management	Consent	1 year
Council contact details	Email address, persons name, address, telephone number	Clerk	Website	Email/hard drive/cloud	Password/encryption	Management	Contract	As long as necessary
Loan applications	Name, address, telephone number, email, bank details	Clerk	To the intended recipient	Hard drive/cloud/filing cabinet	Password/encryption	Management	Contract	3 years
Grant request	Email address, persons name, address	Employee	To grant provider	Hard drive/filing cabinet/cloud/email	Password/encryption	Financial/management	Contract/public interest	3 years
Accident book	Name, address, email address, phone number	Clerk, councillor, employee, contractor, board member	To board/insurers	Hard copy/email	Locked office	Health and Safety	Legal obligation	3 years
Training requests	Email address, persons name, address	Staff, board member	To training provider	Hard drive/email	Password/encryption	Management	Contract	3 years
Legal requests	Email address, persons name	Clerk	To NALC Legal/LGSS Law/Wellers Hedley	Email/hard drive	Password/encryption	Management	Contract	6 years
Surveys	Email address, persons name	Councillor/clerk	To intended recipients	Email/hard drive	Password/encryption	Management	Contract	3 years

HR requests	Name, address, telephone number, email	Councillor/clerk	To HR contact	Email/hard drive	Password/encryption	Management	Contract	6 years
Membership (NALC/SLCC)	Name, address, telephone number, email	CEO	To the intended recipient	Hard drive/email	Password/encryption	Management	Contract	1 year