Electoral Office Northern Ireland
Data Supply Undertaking - Terms

Definitions and Introduction

These Terms set out the arrangements for the safe and secure sharing of data with **You** (the recipient) by **Electoral Office Northern Ireland** (EONI). Definitions are contained in Appendix 1.

Purpose

These Terms relate to the Data referred to in Parts 6 and 7 of the Representation of the People (Northern Ireland) Regulations 2008 ('the Regulations') only ('the Data') and do **not** give unrestricted access to any other information EONI may hold. The data are only available for the named recipients/organisations and should not be shared with a third party.

The Purpose of these Terms is to make the Data available in accordance with Parts 6 and 7 of the Regulations. The Data may only be used in accordance with the Regulations and Data Protection Legislation.

Lawful Basis for Data Sharing

EONI have the power to share the Data with You in accordance with the Regulations.

Data use

- The Data will be provided via a secure site maintained by EONI
- It will be provided within a reasonable period after receipt of a valid request.
- you will ensure the Data provided is only used for the Purpose set out above.
- you should not assume that any non-personal information is not sensitive and can be freely shared
- **EONI reserves the right to make a referral to the Information Commissioner's Office in relation to your compliance with Data Protection Legislation and these Terms.**
- no person to whom this these Terms apply may—
  (a) supply to any person or organisation a copy of the Data
  (b) disclose information contained in it; or
  (c) make use of such information,
  otherwise than in accordance with the Regulations and any enactment as defined in the Regulations.

Requests for information

You must not supply this data to a third party even under a Data Protection Subject Access Request, however you may be subject to Freedom of Information request.

Responsibility for complying with Freedom of Information requests to you falls to you as the Party receiving the request in respect of information they hold. You shall immediately inform the EONI of any request for disclosure. In cases where information sought may be held by EONI, the requester should be advised appropriately.

Compliance with Legislation

You will comply with all principles set out in Data Protection Legislation in all your processing and in particular will ensure that the Data shared is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for those purposes;
- accurate and, where necessary, kept up to date;

- kept in a form which permits identification of Data Subjects for no longer than is necessary to fulfil the stated purpose; and
- processed securely at all times.

You are responsible for ensuring you meet the conditions set out in the Data Protection Legislation, the Regulations, any other relevant enactment and these Terms when processing personal information.

You will ensure that Staff are only given access to the Data where there is a legal right for them to have such access.

You are responsible for ensuring that any Staff accessing the Data under these Terms follow the procedures and standards that have been agreed and incorporated within these Terms.

You are responsible

- for ensuring that any Staff accessing the Data under these Terms are trained and fully aware of their responsibilities under Data Protection Legislation to maintain the security and confidentiality of personal Data.
- You are responsible for ensuring that any Staff accessing the Data under these Terms are trained and fully aware of their responsibilities under the Regulations.
- You assume Data Controller responsibility on receipt of the Data and will process it strictly in accordance with the purpose set out in these Terms and the Regulations.
- You confirm that you have a suitable Data Breach Management Policy in place and will share same if so requested by EONI.

Security
You will take appropriate technical and organisational measures against unauthorised or unlawful processing of the Data and against accidental loss of, destruction of, or damage to the Data. Such technical and organisational measures shall ensure that the Data is stored with the proper safeguards at all times to prevent unauthorised access and include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 2 below.

Retention and disposal
The Data shall be retained and stored in compliance with Data Protection Legislation and the Regulations. Data will be destroyed by You when no longer required.

Security incidents or Data breaches
You will:

- comply with your obligations under Data Protection Legislation, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and comply with Data Guidance.
- acknowledge that when you have received Data under these Terms you will be responsible for ensuring that your own Processing of that Data complies with this clause;
- use the Data shared solely for the purposes identified and shall not process the Data for any other purposes;
- agree to treat the Data received under these Terms as confidential and shall safeguard it accordingly. Respect for the privacy of individuals will be afforded at all stages of processing;
- reflect the Data sharing in your Privacy Notices or those of any party or body;
- notify to EONI any breach of these Terms connected to the sharing of Data as soon as possible and at least within 24 hours of first suspecting the breach. This obligation extends to breaches concerning the systems on which the Data shared are held, even if the Data shared is not directly affected;

- promptly notify EONI of any complaint received from any person about the sharing of Data under these Terms or any correspondence from the Information Commissioner or other regulator regarding the sharing of Data under these Terms; and
- assist EONI, in responding to requests made under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 in relation to the Data shared under these Terms to ensure a co-ordinated and consistent response.
- allow EONI to request that an investigation covering containment and recovery, assessment of risks, notification of breach and evaluation and response in line with appropriate data breach management guidelines and recommendations be undertaken within a defined time limit and shared with EONI.

Indemnity
In the event of a breach of these Terms which results in a financial penalty, claim or proceedings, You agree to co-operate to identify and apportion responsibility for the breach and to indemnify, defend and hold harmless EONI from and against all and any losses, claims, liabilities, costs, charges, expenses, awards and damages of any kind including any fines and legal and other professional fees and expenses (irrespective of whether they were reasonably foreseeable or avoidable) which it/they may suffer or incur as a result of, or arising out of or in connection with, any breach by you of any of your obligations in these Terms.

Remedies and no waiver
The rights and remedies provided under these Terms are in addition to, and not exclusive of, any rights or remedies provided by law or in equity.

A waiver of any right or remedy under these Terms or by law or in equity is only effective if given in writing and signed on behalf of the Party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.

A failure or delay by EONI in exercising any right or remedy provided under these Terms or by law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under these Terms or by law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

Electoral Office for Northern Ireland
November 2023

APPENDIX 1: DEFINITIONS

In these Terms the following words have the following meanings:

Controller	As defined in the Data Protection Act 2018
Data Guidance	Any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in these Terms or not). This includes but is not limited to guidance issued by the European Data Protection Board and the Information Commissioner.
Data Protection Legislation	Means the Data Protection Act 2018, the UK General Data Protection Regulation, all applicable Law concerning privacy, confidentiality or the Processing of Personal Data including but not limited to the Human Rights Act 1998, the common law duty of confidentiality and the Privacy and Electronic Communications Regulations
Data Subject	As defined in the Data Protection Act 2018
Data	Personal data as defined in the Data Protection Act 2018
Process/Processor	As defined in the Data Protection Act 2018
Party	A party to these Terms
Regulatory or Supervisory Body	Means any statutory or other body having authority to issue guidance, standards or recommendations relevant Party and/Staff must comply with or to which they must have regard.
Staff	Any person or persons, including service technicians who shall from time to time, permanently or temporarily, work under the direction or supervision of any Party to these Terms or shall be engaged by or render services to the Party either as employee, contractor, operator, representative and or agent.

APPENDIX 2: COMPLIANCE WITH LEGAL &PRACTICAL SECURITY REQUIREMENTS

1. **Legal requirements**
1.1 The Processor shall, in respect of the processing of personal Data on behalf of the Controller, identify and comply with any specific security provisions imposed by the Controller's national law.

2. Practical security measures
2.1 In compliance with its obligations under section 3 below with regard to the processing of personal Data on behalf of the Controller, the Processor, as a minimum requirement, shall give due consideration to the following types of security measures:
2.1.1 Information Security Management Systems;
2.1.2 Physical Security;
2.1.3 Access Control;
2.1.4 Security and Privacy Enhancing Technologies;
2.1.5 Awareness, training and security checks in relation to personnel;
2.1.6 Incident/Response Management/Business Continuity; and
2.1.7 Audit Controls/Due Diligence;

The Processor shall adopt, as a minimum, the security measures outlined below.

3.1 Physical Security
• Fit appropriate locks or other physical controls to the doors and windows of rooms where computers are kept.
• Physically secure unattended laptops (for example, by locking them in a secure drawer or cupboard).
• Ensure you control and secure all removable media, such as removable hard-drives, CDs and USB drives, attached to business-critical assets.
• Destroy or remove all business-critical information from media such as CDs and USB drives before disposing of them.
• Ensure that all business-critical information is removed from the hard drives of any used computers before disposing of them.
• Store back-ups of business-critical information either off-site or in a fire and water-proof container.

3.2 Access Controls
• Use unique passwords, that are not obvious and change them regularly, preferably at least every three months.
• Use passwords that contain letters in both upper and lower cases, numbers and special keys, and are six or more characters in length.

3.3 Security and Privacy Technologies
- Ensure that all devices used have anti-virus software installed, and the virus definitions must be updated at least daily. At least once a month, devices must be scanned for viruses.
- Where devices are connected to the Internet, they must be protected by a software/hardware firewall.
- Data should be protected as it transits from the device to any services the device uses.
- Data stored on the device should be satisfactorily encrypted when the device is in its "rest" state.
- The device has the latest operating system, and application security patches applied.
- A unique username and complex password is used to access the device

3.4 Awareness, training and security checks in relation to personnel
• Perform integrity checks on all new employees to ensure that they have not lied about their background, experience or qualifications.

• Give all new employees a simple introduction to information security and ensure that they read and understand your information security policy. Ensure employees know where to find details of the information security standards and procedures relevant to their role and responsibilities.
• Ensure that employees have access only to the information assets they need to do their jobs. If employees change jobs, you must ensure that they do not retain access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
• Ensure that no ex-employees have access rights to your systems.
• Ensure that additional security measures are put in place where employees are working remotely
• Ensure employees know about the common methods that can be used to compromise your system.

3.5 Incident/Response Management/Business Continuity
• Ensure that employees understand what is meant by a Security Incident. A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business–critical information or systems.
• Ensure that employees are trained to recognise the signs of Security Incidents.
• Ensure that employees receive training on the need to notify anything which may be a sign of a Security Incident and are kept informed as to the identity of the person to whom such notifications should be made.
• Ensure that if a Security Incident occurs, employees know who to contact and how.
• Have in place a plan to assure business continuity in the event of a serious Security Incident (a "Business Recovery Plan"). The plan should specify:

- Designated people involved in the response;
- External contacts, including law enforcement, fire and possibly technical experts;
- Contingency plans for foreseeable incidents such as: o Power loss; o Natural disasters and serious accidents; o Data compromise; o No access to premises; o Loss of essential employees; o Equipment failure;

• Ensure that your Business Recovery Plan is issued to all employees and is tested at least once a year, regardless of whether there has been a Security Incident.
• After every incident when the plan is used, and after every test, re-examine and update the Business Recovery Plan as necessary using the lessons learned.

3.6 Audit Controls/Due Diligence Ensure that you have in place appropriate security audit arrangements including:
• Auditing of who has access to its system (in general and in relation to particular types of information);
• Logging of such access to the system; and
• Auditing of compliance with security procedures.