Northern Ireland Community Relations Council

Data Protection Policy and Procedures

May 2018

DOCUMENT CONTROL

The Current status of the document is issued Final.

Version No.	Approval by	Approval date	Issue date
One	Board	6th June 2018	6th June 2018

THE COMMUNITY RELATIONS COUNCIL DATA PROTECTION POLICY AND PROCEDURES

1. FOREWORD

This policy and supporting procedures will inform Community Relations Council employees and those Board members about the key data protection issues, including General Data Protection Regulation (GDPR). It sets out information needed to ensure that the Community Relations Council complies with its data obligations and reference further guidance should that be necessary. .

This policy and supporting procedures aim to ensure that all staff, stakeholders and third parties are aware of both their Data Protection rights and responsibilities including those arising from GDPR and to minimize the risk to the Northern Ireland Community Relations Council (CRC) of any Data Protection potential breaches.

All staff have a part to play in managing personal information safely, so are required to read this policy. The Data Protection Officer is also available to provide further advice to ensure that CRC complies with the GDPR.

Thank you.

2. THE COMMUNITY RELATIONS COUNCIL DATA PROTECTION POLICY

Statement of Policy

The Community Relations Council is fully committed to ensuring personal data is managed in accordance with the provisions of the General Data Protection Regulation (GDPR).

This policy relates to all personal data held by the Community Relations Council. The types of personal data that CRC may be required to handle include information about

- past and present employees;
- past and present board members;
- employees of funded groups;
- suppliers;
- bodies who have applied for grants and
- others that it works with, advises or supports.

All personal data, held by the Community Relations Council, whether as computerised records or as well as manual filing systems, is subject to the safeguards set out in the GDPR. This policy sets out how the CRC will process that personal information to enable us to perform its functions in accordance with the GDPR.

Privacy by Design, Data Minimisation and Pseudonymisation are key to Community Relations Councils approach to data protection. In order to demonstrate best practice and compliance with the GDPR, the ICO advises that privacy and data protection is a key consideration in the early stages of policy development and then throughout its lifecycle. Adhering to the concepts of Privacy by Design, Data Minimisation and Pseudonymisation will help the CRC comply with its obligations under legislation.

Policy Awareness

All employees will be made aware of the CRCs Data Protection Policy Statement and Procedure Data Protection by their line managers, and are expected to read and understand this policy and if they require clarification contact the Data Protection Officer for advice. This policy will be made available in written format, electronic format and published on the CRC website.

This policy applies to all employees of CRC, whether permanent or temporary, and workers, casual staff, agency staff and volunteers when working in or for CRC. It also includes all members of the CRC Board when acting in that capacity.

All managers and employees have responsibilities for complying with the requirements of the GDPR by ensuring they process personal data in line with the data protection principles set out in Section 4.

Responsibilities

The Chief Executive Officer (CEO), as the Accounting Officer, has overall responsibility for the Data Protection Policy. The Director of Finance, Administration and Personnel, in the role of the Data Protection Officer is responsible for developing and enforcing information and records management practices. The Audit and Risk Assurance Committee provides oversight on behalf of the Board.

Changes to the Policy

The CRC reserves the right to change this policy at any time.

3. BACKGROUND

The GDPR aims to protect privacy and prevent data breaches. Personal data means any information that relates to an identified or identifiable living person. It may include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion, or sexuality.

It can also include an individual's email address or job title if that sufficiently picks them out so that they can be identified (in isolation or with other information that may be held). The above is not exhaustive and any information that relates to an individual can be personal data.

The GDPR gives protection for personal data, and imposes obligations on those who process personal data.

Controllers and Processors

- "Data controller" is defined as a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

- "Data processor", in relation to personal data, is defined as a person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.

- "Processing", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. What this means is that even storing and holding information is categorized as "processing" under the GDPR. Both Data Controllers and Data Processors carry our Processing.

The definition of 'processing' suggests that a data processor's activities must be limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure. Activities such as interpretation, the exercise of professional judgement or significant decision - making in relation to personal data must be carried out by a data controller.

In most present cases where the Community Relations Council processes personal information, the Community Relations Council will be the Controller.

The GDPR provides the following rights for individuals:

1 The right to be informed.

2 The right of access.

3 The right to rectification.

4 The right to erasure.

5 The right to restrict processing.

6 The right to data portability.

7 The right to object.

8 Rights in relation to automated decision making and profiling.

The Community Relations Council develops its policies and procedures to ensure that the above rights granted to individuals by GDPR are protected.

4. DATA PROTECTION PRINCIPLES

The GDPR is underpinned by a set of six data protection principles that require personal data to be processed in such a way as to embed the concept of privacy by design.

1. Lawful, fair and transparent

There has to be legitimate grounds for collecting the data and it must not have a negative effect on the data subject or be used in a way they wouldn't expect.

2. Limited for its purpose

Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.

3. Adequate and necessary

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected. CRC will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

4. Accurate and Up to Date

Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.

5. Not kept longer than needed

Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

6. Integrity and Security

Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction, and kept safe and secure.

5. DATA SECURITY AND RISK MANAGEMENT

The Community Relations Council will process all personal data it holds in accordance with its Information Security Policy and other Information Governance Policies.

The Community Relations Council is the data controller for the data it requests and processes from the data subjects. Sometimes the Community Relations Council asks other organisations to process the data on its behalf; these organisations are the data processors for CRC.

Data Privacy Impact Assessments (DPIA)

Data Privacy Impact Assessments (DPIAs) are an integral part of how the Community Relations Council delivers Privacy by Design, Data Minimisation and Anonymization, together with other GDPR obligations are embedded in the Community Relations Council approach to policy and procedure development.

Data protection risk is unique in that CRC must manage its own corporate risk as well as risk to the data subjects. DPIAs are a tool that is used to identify and mitigate privacy risks of projects as well as corporate risk. DPIAs can help design more efficient and effective processes for handling personal data, and thus reduce the risk to CRC as an organisation and the data subject.

Conducting a DPIA is the most effective way to demonstrate that personal data processing complies with the GDPR. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used, where this is possible, and devising more straightforward processes for staff.

A DPIA must be completed before beginning a new project, drafting a new or revising an existing procedure, drafting a new or revising an existing policy, when preparing a business case or issuing an invitation to tender. Each DPIA must be reviewed and approved by the DPO before progressing the associated work any further. Should expenditure expected to be less than £5k but will involve personal data, the project must be reviewed and approved by the DPO, who may make relevant recommendations.

The Community Relations Council Data Privacy Impact Assessments template is included in Appendix 6.

An Overview of Data Privacy Risk

Examples of Data Protection risks to Community Relations Council and the Data Subject are

RISK	Data Subject	CRC
Financial Loss	X	
Financial Penalties		X
Loss of personal data	X	X
Breach of legislation		X
Loss of reputation	X	X
Incorrect decision based on inaccurate data	X	

Examples of where control weakness that fail to mitigate data privacy risk include:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Key considerations in designing privacy into CRC procedures that determine the appropriate approach to minimising risk include:

- deciding not to collect or store particular types of information;
- ensuring that information is minimised and held in the appropriate format;
- ensure that procedures require personal data to be anonymised wherever possible;
- applying up to date retention schedules;
- ensuring that staff are properly trained and are aware of potential privacy risks;
- ensuring that the appropriate legal basis for processing is applied the data subjects are suitably informed; and
- ensuring that GPDR compliance third party agreements are in place.

6. LAWFUL BASIS FOR PROCESSING

The Lawful Basis for processing personal information must be determined before processing can begin. At least one of the following must apply:

Consent	The individual has given clear consent for you to process their personal data for a specific purpose.
Contract	The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal obligation	The processing is necessary for you to comply with the law (not including contractual obligations).
Vital interests	The processing is necessary to protect someone's life.
Public task	The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate interests	The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

It is important to get this right first time. If the Community Relations Council find at a later date that its chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

Factors to consider include:

- What is CRCs purpose in processing this information
- What is CRC trying to achieve?
- Can CRC reasonably achieve it in a different way?
- Does CRC have a choice over whether or not to process the data?

While CRC does not perform tasks set down in UK Law, it is a public authority for the purposes of Section 75 (Equality Legislation), the Freedom of Information Act, has an Accounting Officer, is subject to Managing Public Money NI and has a Management Statement/Financial Memorandum in place with The Executive Office. Therefore this policy places the Community Relations Council within the definition under Article 6 (1) of a Public Authority. The Community Relations Council will apply the Public Task lawful basis whenever it is appropriate to do so.

Correspondingly it would be inappropriate for the Community Relations Council to use legitimate interest as the Lawful Basis and will not do so.

The lawful basis for processing and the basis for assigning that basis is documented by the Data Protection Officer and approved by the CEO. The record of the lawful basis will be updated by the Data Protection Officer as required but will be reviewed at least once per year.

7. RIGHT TO BE INFORMED

The Community Relations Council will provide privacy information to individuals including:

- the purposes for processing their personal data;
- retention periods for that personal data and
- who the Community Relations Council will be shared with.

Where possible this will be provided at the point of collection. Where the Community Relations Council obtains personal data from other sources, such as grant claims, the Community Relations Council will make arrangements to provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

The Community Relations Council will maintain a Privacy Notice on its website. The Privacy Notice will contain, as a minimum, the information shown in the table below and will be reviewed annually.

Name and contact details	The categories of personal data obtained
The contact details of the DPO	The recipients or categories of recipients of the personal data
The purposes of the processing	The details of transfers of the personal data to any third parties
The lawful basis for the processing	The retention periods for the personal data
The source of the personal data	The rights available to individuals in respect of the processing
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	The details of the existence of automated decision-making, including profiling

When the Community Relations Council collects personal data it will provide a copy of its privacy statement at the time, or in advance of, the Community Relations Council obtains the data. When The Community Relations Council obtain personal data from a source other than the individual it relates to, Community Relations Council will arrange for the individual to be provided with the privacy information. The table below summarises how privacy information will be communicated to the Community Relations Council's main groups of data subjects

Employees of Funded Groups	Through Data Sharing Agreement. The Funded group will be required to notify affected employees and direct them to Community Relations Council's privacy notice.

Community Relations Council employees	Through employee contracts and agreements
Newsletter recipients	Link to Privacy Notice on newsletter.
Consultations	Link to Privacy Notice on consultations.
Other Communications	Link to Privacy Notice on emails and Community Relations Council letter templates.

8. DATA PROTECTION OFFICER

The GDPR introduces a duty for Community Relations Council to appoint a Data Protection Officer (DPO) for public authorities.

The role of the DPO is to assist the Community Relations Council to monitor internal compliance, inform and advise on the Community Relations Council's data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The DPO's tasks are defined in Article 39 and in ICO guidance as being:

- to inform and advise employees about obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR, other data protection laws, and internal data protection polices;
- to advise on, and to monitor, data protection impact assessments;
- to be the first point of contact for supervisory authorities and for individuals whose data is processed and
- to take into account the risk associated with processing the Community Relations Council is undertaking. The DPO must have regard to the nature, scope, context and purposes of the processing.

Where those charged with governance decide not to follow the advice given by the DPO, they should document their reasons to help demonstrate accountability.

It is assumed that the roles and responsibilities of the DPO will sit in the office of the Director of Finance, Administration and Personnel. The Community Relations Council recognises that the Director of Finance, Administration and Personnel is also a Data Controller, creating conflict of interest with their role as DPO. Given the size of the Community Relations Council there is no way for the organisation to avoid this risk while assigning the role of DPO to a post with sufficient competencies and access to carry out the function. As a mitigating control the DPO will log and report all data protection events and report these to the CEO and Audit and Risk Assurance Committee. This log will be available for internal audit review.

9. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

The Community Relations Council sometimes needs to share information with other organisations, for example, if:

- it is under a duty to disclose or share a data subject's personal data in order to comply with any legal or regulatory requirements;
- to enforce or apply any contract with the data subject or other agreements with whom the data subjects have an agreement; or

- to protect rights, property, or safety of staff, board members, stakeholders, suppliers or others (including those that it works with, advises or supports).

Any third parties who are users of personal information supplied by CRC will be required to confirm and demonstrate that they will abide by the requirements of the GDPR. This will be evidenced by use of a Third Party Processing Agreement. Audits may be carried out at any time by CRC to ensure compliance.

Where a third party is processing data on behalf of the Community Relations Council, the third party agreement will be a Data Processor and therefore a third party agreement will be required. That agreement will identify the following in relation to data processing:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject and
- the obligations and rights of the controller.

The third party agreement will include the following requirements from the processor:

- To only act on the written instructions of the controller;
- To ensure that people processing the data are subject to a duty of confidence;
- To take appropriate measures to ensure the security of processing;
- To only engage sub-processors with the prior consent of the controller and under a written contract;
- To assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- To assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- To delete or return all personal data to the controller as requested at the end of the contract; and
- To submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In certain circumstances, information relating to employees acting in a business capacity may be made available provided:

- we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the employee has consented to the disclosure; or
- the information is in a form that does not identify individual employees.

The ICO have provided checklists for 'systematic data sharing' and 'one-off requests' in their Data Sharing Code of Practice, which are particularly helpful when starting a new project or programme which may involve sharing of personal data.

A sample third party processing agreement and third party confidentiality agreement are attached as appendices to this policy.

Confidentiality must be respected, where appropriate. Employees within CRC should not disclose personal information to any third party, unless they believe it is fair and lawful to do so.

10. RETENTION OF DATA

The CRC holds different types of information for different lengths of time, depending on the legal and operational requirements. The CRC will keep some forms of information longer than others in line with financial, legal or archival requirements.

The Community Relations Council maintains a Records Management and Document Retention policy with supporting procedures that provide a list of retention periods and provides guidance on maintenance of CRC's Information Asset Register. Information will not be held for any longer than is needed and personal information will be clearly identified.

11. SUBJECT ACCESS REQUEST

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The Community Relations Council will provide a copy of the information free of charge. However, CRC will charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

The information will be provided without delay and at the latest within one month of receipt. If the request is complex or numerous the Community Relations Council will extend the period of compliance by a further two months and will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The Community Relations Council will verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, you should provide the information in a commonly used electronic format.

Detailed guidance on complying with a Subject Access Request is set out in Appendix 4. The Data Subject seeking access to their information may use the Subject Access Request Form shown in appendix 5.

12. PROVIDING ACCESS TO INDIVIDUAL RIGHTS

As noted under Section 3 the GDPR gives data subjects' eight specific rights to their personal data. The GDPR introduces the obligation from organisations to have procedures in place to ensure that those rights can be exercised on request.

The Right to Access is consider under Section 10: Subject Access Request above. The remaining seven rights are considered below.

Right to Rectification

The GDPR gives individuals the right to have inaccurate personal data rectified and to have incomplete personal data completed. Even where the Community Relations Council have implemented effective internal control to ensure that accuracy and completeness of personal data the GDPR creates the obligation for the data controller to consider accuracy upon request.

Right to Erasure

The Community Relations Council will erase personal data of individuals where the following conditions are met:

- the personal data is no longer necessary for the purpose originally collected or processed
- where consent is the lawful basis for holding the data, and the individual withdraws that consent
- processing the personal data for direct marketing (e-newsletter) purposes and the individual objects to that processing;
- the Community Relations Council has processed the personal data unlawfully;
- you have to do it to comply with a legal obligation;

Right to Restrict Processing

The Community Relations Council will restrict processing of personal data of individuals where one of the following conditions are met:

- the individual contests the accuracy of their personal data while the Community Relations Council is verifying the accuracy of the data;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- the Community Relations Council no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or

As there are close links between the Right to Erasure, the Right to Restrict and the Right to Object the Community Relations Council, as matter of good practice will automatically restrict the processing whilst it is considering the accuracy or the legitimate grounds for processing the personal data in question
The Community Relations Council will consider the following steps when complying with a request to restrict processing:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from distribution lists.

The Community Relations Council will not process the restricted data in any way except to store it unless:

- The Community Relations Council has the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal) or
- it is for reasons of important public interest.

Right to Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract and
- when processing is carried out by automated means.

Right to Object

The right to object allows Individuals have the right to object to:

- processing based on the performance of a task in the public interest/exercise of official authority;
- direct marketing and
- processing for purposes of scientific/historical research and statistics.

When an objection is received where personal data is processed due to a public task the Community Relations Council will stop processing the personal data unless the DPO can demonstrate:

- compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- or the processing is for the establishment, exercise or defence of legal claims.

Where the Community Relations Council processes personal information for the performance of a public task it will inform individuals of their right to object "at the point of first communication" and in its privacy notice.

When an objection is received where the Lawful Basis is consent, such as the e-newsletter, the Community Relations Council will interpret this as consent being withdrawn and cease to process immediately. There are no exemptions or grounds to refuse.

Rights related to automated decision making including profiling

At present the Community Relations Council does not make automated decisions. Should this change the Community Relations Council will update its procedures accordingly.

Complying with a request to exercise Individual Rights

On receipt of a request the Community Relations Council will take all reasonable steps to ensure that the data subject's rights are exercised. What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important the right is, the personal data and the data subject, the greater the effort Community Relations Council will make delivering that individuals right.

The GDPR allows an individual to make a request to exercise their rights in writing and to any part of Community Relations Council or person within Community Relations Council. Furthermore a request to does not need to mention the right being exercised. For example, if an individual has challenged the accuracy of their data and has asked for it to be corrected, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request. A record of all requests is maintained by the DPO.

All requests must be reported immediately to the Data Protection Officer. The DPO will prepare a plan within 72 hours detailing what steps the Community Relations Council will take to comply with the

request. The Community Relations Council will comply within one calendar month of the request being received unless there are exceptional circumstances. Should exceptional circumstances exist, the Data Subject will be notified and a report made to the Audit and Risk Assurance Committee.

A fee cannot be charged.

The Community Relations Council will restrict processing of personal data during the period when the accuracy of personal data is being checked or updated

The Data Protection Officer will write to the individual once the extent of accuracy of personal data has been established and rectified.

In certain circumstances the Community Relations Council can refuse to comply with a request to correct personal data. Should these circumstances apply the DPO will report to the CEO explaining why they apply and what action should now be taken. The decision not to comply must be approved by the CEO and reported to the Audit and Risk Assurance Committee.

13. DATA BREACH

A data breach is defined by GDPR as "any unauthorised or unlawful processing, accidental loss or destruction of, or any damage to, personal information held by CRC in both electronic and paper copy".

Data breach incidents should be reported to the DPO verbally by the CRC employee who becomes aware of the data breach as soon as the data loss has been discovered. A formal breach report form as shown in Appendix 3, should then be immediately completed by the CRC employee who becomes aware of the data breach. The completed form should be forwarded to the DPO without delay.

Such incidents will be reported to the Information Commissioner's Office within 72 hours and to the data subject as soon as possible.

How to respond to a data breach

Whilst breaches should be escalated immediately (even if all the details are not yet clear), it is important that staff also bring any 'near miss' incidents or information security weaknesses to the attention of their line manager. If you become aware that data security has been breached you must inform your line manager immediately. The line manager in turn must advise the Data Protection Officer, who will assess the severity of the incident and notify the CEO. The CEO and the DPO will together agree a way forward.

The Data Protection Officer must report the breach to the ICO within 72 hours of CRC becoming aware of the breach and also inform the data subject without delay.

The DPO will present a report on the incident, including:

- summary of the event and circumstances;
- type and amount of personal data affected;
- actions taken by recipient who received the information;
- actions taken to retrieve information and respond to the breach;
- procedures in place to mitigate risk and why not effective;
- details of notification to affect data subject(s);
- has a complaint been received from a Data Subject?
- assessment of risk to data subject and CRC with proposed mitigating actions;
- details of communication with ICO;
- proposed changes to procedure to reduce risks of repeat and
- reporting and other recommendations.

This report will be presented to the CEO as soon as possible and no more than 10 working days from the date of the incident and a summary report will be provided to the Audit and Risk Assurance Committee. Should an ARAC meeting take place before the report is complete the committee should be briefed on the incident at the earliest opportunity.

The DPO will also update the ICO on the progress of the report and the conclusions and procedure and policy changes identified to reduce the risk of a repeat data security breach.

The breach will be notified to the TEO and formally reported through the quarterly assurance statement.

In the event of a near miss, the Data Protection Officer should initiate an investigation in order to ensure weaknesses are addressed, and lessons learned are disseminated. The Data Protection Officer will set a timeframe for an investigation to allow him/her to provide a short report to the CEO within fifteen working days. The CEO and the DPO will then together agree a way forward and decide on whether or not there is an operational need to report the near miss as per the steps outlined above.

14. THE ROLE OF THE INFORMATION COMMISSIONER'S OFFICE

The Information Commissioner's Office (ICO) has a range of statutory powers to assess and enforce compliance with the GDPR. The main powers are outlined briefly below.

ICO Register of Data Controllers

The Information Commissioner maintains a public register of data controllers who process personal information. Each register entry includes the name and address of the data controller, and a general description of the type of processing carried out. Notification is the process by which a data controller's details are added to the register. Anyone can consult the register to find out what processing is being carried out by a particular organisation.

The GDPR requires CRC to notify the Information Commissioner's Office (ICO) on an annual basis. Prior to the expiry of the registration, the Data Protection Officer will request all business areas to closely examine the CRC's current notification details and advise of any additions or amendments required for the incoming year.

Managers must ensure that the purposes and purpose descriptions set out in the CRC's notification fully cover all the processing of personal information taking place within their business area. The Data Protection Officer must be informed immediately if any new type of personal information is to be processed, or if a type of personal information is no longer to be processed. This will allow the CRC's notification to be amended as required by data protection legislation.

Failure to amend a record within 28 days of discovering the need for a change is a criminal offence so it is vital that all areas carry out this exercise every year and that our registration details with the ICO are kept up to date.

CRC's entry number on the Information Commissioner's Data Protection Register is Z5024924 and can be viewed online.

15. CHILDREN

Children merit specific protection when processing their personal data. The Community Relations Council will develop and maintain clear privacy notice to read by Children. The Community Relations Council will ensure that children have the same rights as adults over their personal data.

Where CRC rely upon Public Task as its lawful basis for processing Community Relations Council will balance the public interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. The Community Relations Council will take appropriate measures to safeguard against those risks.

The Community Relations Council will seek to avoid the processing of Children's personal data However, where this is no longer possible the written summary must be sent to the Data Protection Officer before the Community Relations Council become is responsible for processing Children's personal data. The report must include the following:

- subject matter of the personal data to be processed;
- duration of the processing;
- nature and purpose of the processing;
- type of Personal Data;
- categories of Data Subject;
- how the Child/Guardian will be notified.

The Data Protection Officer will then draft a report to the Chief Executive Office recommending whether or not it would be appropriate to hold personal data of children as proposed, the lawful basis for doing so and clearly detailing the additional procedures to ensure the rights of children are protected.

APPENDIX 1 **GLOSSARY OF TERMS**

Definitions

The following definitions are used in this policy and shall mean the following:

Consent	the individual has given clear consent for you to process their personal data for a specific purpose.
CRC	Northern Ireland Community Relations Council
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Concerning Health	any personal data relating to the physical or mental health of an individual or the provision of health services to them
Data controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. CRC is the data controller of the personal data used in the CRC
Data Erasure	also known as The Right to be Forgotten, it entitles the data subject to have the data controller erase his or her personal data, ease further dissemination of the data and potentially have third parties cease processing of the data
Data Portability	the requirement for data controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller and allows for the transfer of the personal data to that other data controller
DPIA	Data Privacy Impact Assessment, a process which enables organisations such as CRC to identify and reduce the privacy risks of any particular project. Also known as a PIA.
Data Processors	includes any person or organisation that is not a data user that processes personal data on CRC's behalf and on its instructions. Staff of data controllers are excluded from this definition but it could include suppliers which handle personal data on CRC's behalf, for example companies who store our information backups.

Data Protection Authority	national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the European Union. Also known as a Supervisory Authority
Data Protection Officer	an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures needed to be compliant with the GDPR. Also known as DPO.
DSA	Data Sharing Agreement. Agreement between two or more parties for the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation
Data Subject	a natural person whose personal data is processed either by a data processor or a data controller
Data Users	are those staff whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and the Security Policies.
Encrypted Data	personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
Filing System	any means of categorizing data that makes it accessible according to specific criteria, or able to be queried
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
PECR	Privacy and Electronic Communications Regulations 2003
Personal Data	means data relating to a living individual who can be identified from that data (or from that data and other information in its possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Privacy by Design	a principle that calls for the inclusion of data protection principles from the onset of the designing of systems, rather than as an addition at a later stage
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Profiling	any automated processing of personal data without the input of a person, intended to evaluate, analyse or predict the behaviour of a data subject
Pseudonymisation	the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure that it cannot be attributed to the data subject
Recipient	entity to which personal data is disclosed
Right to be Forgotten	also known as Data Erasure, it entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data and have third parties cease processing of the data
Right to Access	also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a data controller has concerning them
SAR	Subject Access Request. Request from an individual to see their own data under the rights given to them in the GDPR

Supervisory Authority	a public authority established by a member state of the European Union in accordance with Article 46 of the GDPR, which is tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the European Union
Special Category Data	includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

APPENDIX 2 **PRIVACY NOTICE**

Community Relations Council

Introduction

At the Northern Ireland Community Relations Council, we're committed to protecting and respecting your privacy.

This Policy explains when and why we collect personal information, how we use it and the conditions under which we may disclose it to others.

Any questions regarding this Policy and our privacy practices should be sent by email to infro@nicrc.org.uk or by writing to

Community Relations Council

2nd Floor

Equality House

7-9 Shaftesbury Square

Belfast

BT2 7DP

About

This privacy notice explains how the Northern Ireland Community Relations Council ("we", "our", "us") (CRC) collects, uses and shares your personal data, and your rights in relation to the personal data we hold. This privacy notice concerns our processing of personal data of past, present and prospective employees, clients and supporters of CRC ("you", "your"). We also have a separate Privacy Notice which applies to employees, workers and contractors.

Northern Ireland Community Relations Council is the data controller of your personal data and is subject to the General Data Protection Regulation (the "GDPR").

How we collect your information

We may collect your personal data in a number of ways, for example:

- when you apply for a grant from CRC and complete grant application forms;
- when you communicate with us by telephone, email or via our website, for example in order to make enquiries or raise concerns;
- in various other ways as you interact with CRC, for the various purposes set out below; or
- from third parties.

The types of information we collect

We may collect the following types of personal data about you:

- your name, and contact information such as address, email address and telephone number, as well as your date of birth, national insurance number (or other tax identification number);
- Your bank account details;
- Car registration;
- Pay roll information; and
- information about your racial or ethnic origin; religion or similar beliefs; and sexual orientation.

How we use your information The purposes for which we may use personal data (including sensitive personal data) we collect during your association with us include to:

- carry out our obligations arising from any contracts entered into by you and us;
- process orders that you have submitted;
- process a grant;
- monitoring equal opportunities;
- administering finance (e.g. for payment of grants, salaries and wages);
- share the CRC E-Newsletter, updates on Together: Building a United Community Engagement Forum, to alert you to re upcoming events and to notify you of the work of Community Relations Council;
- carrying out audits (e.g. to ensure compliance with our regulatory and legal obligations);
- providing operational information (e.g. providing IT support, information about building closures, or safety advice);
- preventing and detecting crime; and
- dealing with complaints, grievances and disciplinary actions.

Funded Groups and their employees

For the performance of a contract we sometimes require access to certain Personal Data relating to employees of groups it funds to for the process grant expenditure claims made by that funded group.

We have put in place a data sharing agreement with each of our funded groups that describes how personal data will be shared, and the principles and procedures that we and the funded group will adhere to when sharing personal data for this purpose. This agreement is available for review from the Community Relations Council website.

The Community Relations Council will not retain or process shared personal data for longer than is necessary to carry out the agreed purposes which shall be documented in the Community Relations Council disposal schedule.

The Community Relations Council has appropriate measures in place to protect the shared personal data in their possession against unauthorised or unlawful processing.

Community Relations stakeholders

The Community Relations Council holds personal data of employees of organisations engaged in or with a corporate interest in peace building activity in Northern Ireland and the work of the Community Relations Council. We use this information to update you on the consultations, community relations stories, updates on Together: Building a United

Community Engagement Forum, to alert you to upcoming events and to notify you of the work of Community Relations Council.

The personal information is held on a secure database with limited access. The database is maintained and updated on an ongoing basis and subject to a detailed review annually.

Other People who contact the Community Relations Council.

If you otherwise engage with the Community Relations Council, including as supplier, an agency worker or to make an enquiry, we may collect personal details depending on the nature of the engagement. Details of retention periods for different aspects of your personal information are available in our retention schedule which is available from Data Protection Officer.

This personal information is held on access controlled secure records database. The database is maintained and updated on an ongoing basis and subject to a regular review.

The basis for processing your information and how we use it

a) Contract

We may process your personal data because it is necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract. In this respect, we use your personal data for the following:

- to interact with you before you receive a grant, as part of the application process (e.g. to send you a grant application pack or answer enquiries about our grants);
- once you have been successful in your grant application, to process the grant and send payment as detailed in our schedule of payments;
- to deal with any concerns or feedback you may have;
- to process payments, including salary payments;
- for any other purpose for which you provide us with your personal data; and
- recovering money you owe to us.

b) Public Task

We may also process your personal data because it is necessary for the performance of our public tasks. In this respect, we may use your personal data for the following:

- to provide you with educational services which may not be set out in our grant agreement but which are nevertheless a part of our mission;
- to maintain and improve the corporate, financial, estate and human resource management of the Community Relations Council;
- to promote equality and diversity throughout CRC; and
- to seek advice on our rights and obligations, such as where we require our own legal advice.

c) Legal Obligation

We may also process your personal data for our compliance with our legal obligations. In this respect, we may use your personal data for the following:

- to meet our compliance and regulatory obligations, such as compliance with anti-money laundering laws and safeguarding requirements;
- for the prevention and detection of crime;
- in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

d) Vital Interest

We may also process your personal data where:

- it is necessary for medical purposes (e.g. medical diagnosis, provision of health or social care or treatment, or a contract with a health professional);
- it is necessary to protect your or another person's vital interests; or
- we have your specific or, where necessary, explicit consent to do so.

e) Consent

We may process your personal date where you have given consent for us to do so. When CRC seeks your consent we will:

- display the request for consent clearly and prominently;
- ask you to positively opt-in;
- give you sufficient information to make an informed choice;
- explain how different ways CRC will use the information,
- provide a clear and simple way for them to indicate they agree to different types of processing; and
- be clear how you can withdraw your consent.

Your rights

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

If you have given your consent and you wish to withdraw it or to exercise any one of the rights listed above, please contact our Data Protection Officer using the contact details set out below. Please note that where our processing of your personal data relies on your consent and where you then withdraw that consent, we may not be able to provide all or some aspects of our services to you and/or it may affect the provision of those services.

Sharing information with others

For the purposes referred to in this privacy notice and relying on the bases for processing as set out above, we may share your personal data with certain third parties. You are given the opportunity to opt out of some of these data sharing arrangements, but you should carefully consider the possible impact of doing this. Unless an opt-out is in place, we may disclose limited personal data to a variety of recipients including:

- our employees, agents and contractors where there is a legitimate reason for their receiving the information,
- third parties who work with us to provide support services (e.g. counselling or payroll services);
- third parties who are contracted to provide IT services for us;
- third parties who are contracted to maintain our database systems;
- internal and external auditors;
- The Executive Office;
- current or potential employers (to provide references);
- other governmental agencies, professional and regulatory bodies (where there is a legitimate reason for disclosure); and
- next-of-kin (where there is a legitimate reason for disclosure).

International Transfer

Personal data may be transferred to countries and organisations outside the European Union that have laws that provide specific protection for personal data and organisations within those countries that provide appropriate protection and redress mechanisms for individuals. Where personal data is transferred outside the EU the Community Relations Council has taken appropriate measures to ensure that your personal information is treated in a way that is consistent with and which respects the EU and UK laws on data protection.

Use of Images

The Community Relations Council may use photographs and/or video taken at its events such as Together: Building a Uniting Community event.

The photographs and/or videos may be used in the following ways:

- The Community Relations Council Website
- The Community Relations Council videos
- The Community Relations Council newsletters

- The Community Relations Council social media channels
- Issuing to the media, including national and local sources for publication
- Issuing to The Executive Office for publication

Photographs and videos will be stored by the Community Relations Council in accordance with this privacy notice.

Changes to your personal data

Please tell us promptly about any changes to the information we hold about you. This is particularly important for your contact details. You can do this by emailing info@nicrc.org.uk.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Cookies and CRC Website

When you visit our website we collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. We do not make any attempt to find out the identities of those visiting our website. We will not associate any data gathered from this site with any personally identifying information from any source. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

How long your information is kept

Subject to any other notices that we may provide to you, we will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention schedule which is available from our Data Protection Officer. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Format and Language

For a copy of this policy in another language or format (such as Braille, audio CD, large print or Easy Read) please contact the Director of Finance, Administration and Personnel. The

CRC will take reasonable steps to accommodate the access requirements brought to the attention of the CRC.

Contact us

If you have any queries about this privacy notice or how we process your personal data, you can contact our Data Protection Officer by email: info@nicrc.org.uk; by telephone: +44 (028) 9022 7500; or by post: Data Protection Officer, Northern Ireland Community Relations Council, 2nd Floor, Equality House, 7-9 Shaftesbury Square, Belfast BT2 7DP.

To request access to the personal data that we hold about you, you may contact our Data Protection Officer by email:info@nicrc.org.uk; by telephone: +44 (028) 9022 7500 ; or by post:

Data Protection Officer

Northern Ireland Community Relations Council,

2nd Floor, Equality House

7-9 Shaftesbury Square,

Belfast

BT2 7DP

Email: info@nicrc.org.uk

Tel: +44 (028) 9022 7500

If you are not satisfied with how we are processing your personal data, you can make a complaint to the Information Commissioner. You can find out more about your rights under data protection legislation from the Information Commissioner's Office website available at: www.ico.org.uk.

Information Commissioner's Office

3rd Floor, 14 Cromac Place

Belfast

BT7 2JB

Tel: 028 9027 8757

Email: ni@ico.gsi.gov.uk

Web: https://ico.org.uk/

APPENDIX 3 THE NORTHERN IRELAND COMMUNITY RELATIONS COUNCIL BREACH OF DATA SECURITY – REPORT FORM

BREACH OF DATA SECURITY REPORT FORM

STAFF REPORT

NAME ……

POSITION

E-mail address …….

A) When did you first become aware of the incident?

B) Provide a description of the incident?

C) How did you become aware of the incident?

D) Confirm that the incident has been reported to your line manager.

E) Have you reported your incident to anyone other than the DPO and your Line Manager?

E) Supporting Documents - Please attach any supporting documentation

SIGNED: ……

DATE: ……

When completed this form should be returned to the Director of Finance, Administration and Personnel in the capacity of the Data Protection Officer, by emailing gmckeown@nicrc.org.uk

Or by post: Mr Gerard McKeown, Director of Finance Administration and Personnel, Northern Ireland Community Relations Council, 2nd Floor, Equality House, 7-9 Shaftesbury Square, Belfast, BT2 7DP.

APPENDIX 4 SUBJECT ACCESS REQUEST AND CHANGE OF DETAILS FORM

THE NORTHERN IRELAND COMMUNITY RELATIONS COUNCIL

CHANGE OF INFORMATION/DELETE DETAILS/SUBJECT ACCESS REQUEST REPORT FORM

NAME ……

ADDRESS ……

……

TELEPHONE …… E-mail address ……

A) Please respond as appropriate:

Please amend my details as below:

……

……

……

Please delete my details YES

Please stop processing my details/change how you process my details as below:

……

……

……

Please transfer my personal information directly to:

……

……

……

Please provide me with copies of the following personal information you hold on me:

……

……

……

Supporting Documents - Please attach any supporting documentation

SIGNED: ……

DATE: ……

When completed this form should be returned to the Director of Finance, Administration and Personnel in the capacity of the Data Protection Officer by emailing gmckeown@nicrc.org.uk

Or by post: Mr Gerard McKeown, Director of Finance Administration and Personnel, Northern Ireland Community Relations Council, 2nd Floor, Equality House, 7-9 Shaftesbury Square, Belfast, BT2 7DP.

APPENDIX 5 **SUBJECT ACCESS REQUEST (SAR)**

Step 1: **Check the request is within the scope of the GDPR**

Determine whether the person's request should be treated as a routine enquiry, or as a subject access request. Any written enquiry that asks for information you hold about the person making the request can be construed as a subject access request, but in many cases there will be no need to treat it as such.

If you would usually deal with a particular type of request in the normal course of business, continue to do so. An example of such a request might be:

- 'I've forgotten my payroll number, what is it please?'

The following are likely to be formal subject access requests:

- 'Please send me a copy of the records you hold on me, as my line manager.'

- 'I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authorisation is enclosed.'

To be within the scope of the GDPR, a subject access request must:

- have been received in writing (including email);

- be a request for information about the applicant ;

- provide sufficient information to verify the data subject's identity and

- provide sufficient information to enable the CRC to locate the information required.

The applicant does not have to quote the GDPR to have the request treated as a formal subject access request.

Step 2: **Who to inform?**

Advise your line manager, Local Information Manager and CRC's Data Protection Officer of receipt of the request immediately.

Step 3: **Verify the identity of the data subject.**

Before disclosing any personal information, you must verify the identity of the data subject. Whilst it is important that you do not send copies of personal information to people who are not the data subject, you must not appear obstructive. The GDPR requires you to take reasonable measures to verify their identity. You should keep a record of what measures you take.

You can often verify their identity from their address or signature. If this is not possible, you can write to the individual asking them to send you a photocopy of some form of identification such as their passport or driving licence.

Step 4: **Clarify the request (if necessary).**

If clarification is required seek advice from the Data Protection Officer and your line manager and write to the person asking for further information.

Step 5: **Calculate deadline for response.**

You have a maximum of one calendar month to respond to a SAR. The clock begins from the date of receipt or date of receipt of proof of identity/further information. Calculate the due date at the outset. Put reminders in your diary, and inform your line manager who will inform the Data Protection Officer.

Step 6: **Open a folder on the shared drive.**

You should open a folder on the shared drive to hold all the information (including email correspondence) relating to the Subject Access Request. This should be in the "Subject Access Requests" folder within the shared drive, and then a separate folder should be opened with the name of the requestor and the nature of the request as the file title.

Example: John Smith Medical Info

- save or scan the request to the folder on the shared drive;

- complete the tracking spreadsheet (available on the shared drive) and

- acknowledge receipt of the request using the standard acknowledgement email/letter format (available on the shared drive).

Step 7: **Search for information.**

Based on the information requested and your knowledge of your business area, decide where personal information about the applicant might be held and locate that information. You may need to search the shared drive, your personnel records and your business area paper records. You may also need to speak to members of your business area and / or other business areas, for example, Departmental HR, to find out if they might hold information about the individual.

The FOI Act means that individuals can make subject access requests for 'unstructured personal data', as well as information held in 'relevant filing systems'. This means that individuals can request any information CRC hold that relates to them. However, if the information is held in an unstructured manner then 'The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004' allows you to refuse the request, where the cost is estimated to exceed the appropriate limit (separate guidance on this is available).

If the CRC does not hold any personal information about the data subject, we must advise the applicant accordingly and we will write to them and let them know.

Step 8: **Review information considering possible exemptions.**

Once you have collected the information you must examine it in detail to establish if it can be released. This must be done on a case by case basis for each individual piece of information. In some cases, you might have to disclose only parts of particular documents and should:

- check that the record is actually about the person concerned and not someone else with the same name;

- screen out any duplicate records;

- only disclose information about the data subject. Where a document contains personal data about others, consider blanking out names (redacting) or contacting the third party to obtain their consent to disclose the record;

- not disclose information which would prejudice the prevention or detection of a crime ;

- not disclose any records which contain advice from our solicitors or where we are asking for legal advice or which were written as part of obtaining legal advice and

- not disclose information which is being used, or may be used in the future, in negotiations with the data subject if the information gives away our negotiating position and disclosing it would weaken our negotiating position.

If there is material that you are concerned about releasing, please contact your Line Manager for advice in the first instance and the Data Protection Officer if you need further assistance.

You can still make routine amendments to personal information after receiving a request. However, you must not make any changes to the records as a result of receiving the request, even if you find inaccurate or embarrassing information. Such action is a criminal offence if it is done after a subject access request has been made. Inaccurate or embarrassing material which does not reflect favourably on the CRC, for example, papers which show that standard procedures were not followed, or the contents of documents which may cause offence to the data subject, should be disclosed. However, you should bring their contents to the attention of the Data Protection Officer to ensure that appropriate action is taken to address any issues they raise.

Step 9: **Prepare response to applicant.**

The applicant should be provided with all personal information relating to them within the scope of their request, that is not exempt and which will not disclose personal information relating to a third party (without their consent). Even when the third party's information should not be disclosed, you should still supply as much as possible by redacting the references to third parties.

The information may include abbreviations or technical terms that the applicant may not understand. You must make sure that they are explained so the information can be understood.

You should liaise closely with the Data Protection Officer to ensure that your response is fully compliant with the GDPR.

Step 10: **Respond to Applicant.**

A copy of the information should be supplied in a permanent form (e.g., photocopy), except where the applicant agrees otherwise; where it is impossible; or, would involve undue effort. This process could include very significant cost or time taken to provide the information in hard copy form. Therefore, an alternative would be to allow the applicant to view the information on screen or in situ.

Please note, individuals can complain to the Information Commissioner's Office or apply to a court if you do not respond within the time limit of one calendar month. Your response should inform applicants of their right of appeal to the Information Commissioner.

A copy of the response must be saved to the folder on the shared drive.

Step 11: **Update the folder on the shared drive.**

The folder must contain:

- update to the tracking spreadsheet
- copies of all correspondence between the CRC, the data subject and any other parties;
- a record of any telephone conversations used to verify the identity of the individual or the information required;
- a record of your decisions and how you came to make them and
- a copy of the response including information sent to the data subject.

Community Relations Council

Diversity Equity Interdependence

The NI Community Relations Council Data Protection Impact Assessment Template

A Data Protection Impact Assessment must be completed before beginning a new project, drafting a new or revising an existing procedure, drafting a new or revising an existing policy, when preparing a business case or issuing an invitation to tender. Each DPIA must be reviewed and approved by the DPO before progressing the associated work any further.

Further guidance is available by contacting the DPO

Step 1: Identify the need for a DPIA: Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Step 2: Describe the Processing
Describe the nature of the processing

Describe the scope of the processing

Describe the context of the processing

Describe the purposes of the processing

Step 3: Consultation process
Consider how to consult with relevant stakeholders:

Step 4: Assess necessity and proportionality (what is lawful basis for processing)

Step 5: Identify and assess risks				
Risk Description	Personal/ Corporate	Likelihood	Impact	Inherent Risk

Step 6: Identify measures to reduce risk				
Risk Description	Actions to mitigate risk	Revised Likelihood	Revised Impact	Residual Risk

Step 7: DPO Review		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted		If overruled, you must explain

or overruled by:		your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX 7 THIRD PARTY PROCESSING AGREEMENT

GENERIC STANDARD GDPR CLAUSES

Notes for completion: The GDPR generic standard clauses may be adapted to fit existing contract templates but you are advised to seek CoPE and/or legal advice when doing this.

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy.

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** take the meaning given in the GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and

resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement.

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Client is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule [X] by the Client and may not be determined by the Contractor.

1.2 The Contractor shall notify the Client immediately if it considers that any of the Client's instructions infringe the Data Protection Legislation.

1.3 The Contractor shall provide all reasonable assistance to the Client in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

Such assistance may, at the discretion of the Client, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Contractor shall provide all reasonable assistance to the Client in providing subject access and allowing data subjects to exercise their rights under the GDPR.

1.5 The client agrees to submit to audits and inspections, including the Client’s designated auditors.

1.6 The client agrees to provide the controller with whatever information it needs to ensure that both the Client and the Contractor are meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the Data Protection Legislation.

1.7 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule [X], unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Client before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are available to be reviewed and approved by the Client as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Contractor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Client or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Client has been obtained and the following conditions are fulfilled:

(i) the Client or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Client;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Client in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;

(e) at the written direction of the Client, delete or return Personal Data (and any copies of it) to the Client on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.8 Subject to clause 1.6 the Contractor shall notify the Client immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1.9 The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Client in phases, as details become available.

1.10 Taking into account the nature of the processing, the Contractor shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Client) including by promptly providing:

(a) the Client with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Client to enable the Client to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Client, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Client following any Data Loss Event;

(e) assistance as requested by the Client with respect to any request from the Information Commissioner's Office, or any consultation by the Client with the Information Commissioner's Office.

1.11 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Client determines that the processing is not occasional;

(b) the Client determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Client determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.12 The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.13 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(a) notify the Client in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Client;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and

(d) provide the Client with such information regarding the Sub-processor as the Client may reasonably require.

1.14 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.15 The Client may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.16 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Client may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

SCHEDULE [X] PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The Contractor shall comply with any further written instructions with respect to processing by the Client.

2. Any such further instructions shall be incorporated into this Schedule.

Description	**Details**
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter].
Duration of the processing	[Clearly set out the duration of the processing including dates].
Nature and purpose of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes]. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment.
Type of Personal Data	[Examples here include: name, address, date of birth, NI Data number, telephone number, pay, images, biometric data etc].
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients students / pupils, members of the public, users of particular website etc. describing how long the data will be retained for, how it be returned or destroyed].
Preventative Measure	Itemised description of control in place to ensure compliance with Data Protection Legislation and to prevent a data breach.

APPENDIX 8 DATA SHARING AGREEMENT

Information Sharing Agreement Contract

This agreement (the "**Agreement**") is made

Parties

1. Community Relations Council. 2nd Floor, Equality House, 7-9 Shaftesbury Square, Belfast BT2 7DP; and

2. _____

_____

_____

Each referred to as a "Party" and together the "Parties".

Background

(1) The following agreement between the Community Relations Council and _____ reflects the arrangements that they have agreed to put in place to facilitate the sharing of Personal Data relating to employees of _____ acting as a data controller, and explains the purposes for which that Personal Data may be used.

(2) As such, _____agrees to share the Personal Data with the Community Relations Council on the terms set out in this Agreement and the Community Relations Council agrees to use the Personal Data on the terms set out in this Agreement.

1. INTERPRETATION

1.1 Definitions:

Agreed Purposes: shall mean those purposes set out in clause 2.2 of this Agreement.

Data Discloser: the Party transferring the Personal Data to the Data Receiver.

Data Protection Law: shall mean (i) the Data Protection Act 1998 until the effective date of its repeal (ii) the General Data Protection Regulation (2016/679) (GDPR) and any national implementing laws, regulations and secondary legislation, for as long as the GDPR is effective in the UK and (iii) any successor legislation to the Data Protection Act 1998 and the GDPR, in particular the data Protection Bill 2017-2019 once it becomes law.

Data Receiver: The Party receiving the Personal Data from the Data Discloser.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

GDPR: the General Data Protection Regulation (2016/679),

Shared Personal Data: the Personal Data and Sensitive Personal Data/Special Category Data to be shared between the Parties under *clause 4 of this Agreement.*

Subject Access Request: has the same meaning as "Right of access to personal data" under GDPR.

Data Controller, **Data Processor**, **Data Subject** and **Personal Data**, **Sensitive Personal Data**, **Special Category Data, Processing, Right to Object and appropriate technical**

and organisational measures shall have the meanings given to them in the Data Protection Law.

2. PURPOSE

2.1 This Agreement sets out the framework for the sharing of **Personal Data** between the Parties as **Data Controllers** and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2.2 The Community Relations Council requires access to certain Personal Data relating to employees of the _____to process grant expenditure claims made by _____.

2.3 The Parties agree that this Agreement formalises a lawful transfer of Personal Data between the Parties and presents no new or additional privacy concerns.

2.4 The Community Relations Council shall not process Shared Personal Data in a way that is incompatible with the Agreed Purposes.

3.0 COMPLIANCE WITH DATA PROTECTION LAW

3.1 Each Party must ensure compliance with the Data Protection Law at all times during the term of The Letter of Offer (REFERENCE) made and to and accepted by_____ on _____DATE.

4. SHARED PERSONAL DATA

4.1 For the purposes of 2.2 the following types of Personal Data may be shared with the Community Relations Council to allow claims to be processed: first name; middle name(s); surname; date of birth; _____email address; personal email address, home address; work mobile phone number, personal mobile phone number, home phone number, car registration; National Insurance Number, pay roll information, and bank account details.

4.2 The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

5. FAIR AND LAWFUL PROCESSING

5.1 Each Party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with clause 2.2 during the Term in accordance with clause 16.1.

5.2 For the purposes of this Agreement, the Community Relations Council shall ensure that it processes Shared Personal Data on the basis that processing is necessary for the following reasons:

(a) for the performance of a contract between the parties;
(b) for compliance with a legal obligation;
(c) for the performance of a task carried out in the public interest and in the exercise of the Community Relation Council's official authority.

5.3 _____undertakes to inform Data Subjects of the purposes and lawful basis for which it will share their Personal Data and provide all of the information that it must provide in accordance with Data Protection Law, to ensure that the Data Subjects understand how their Personal Data will be processed by the Community Relations Council.

6. DATA SUBJECTS' RIGHTS

6.1 Data Subjects have the right to obtain certain information about the processing of their Personal Data through a Subject Access Request. Data Subjects may also request rectification, erasure, to restrict processing, portability and the right to object.

6.2 The Parties agree that the responsibility for complying with a Subject Access Request falls to Party receiving the Subject Access Request in respect of the Personal Data held by that Party.

6.3 The Parties agree to provide reasonable and prompt assistance in line with its Data Protection Policy and Data Protection Law as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other requests, queries or complaints from Data Subjects.

6.4 The Community Relations Council will maintain a Privacy Notice on its website that describes how the CRC collect personal information, the types of information the Community Relations Council will collect, how Community Relations Council use personal information, the basis for processing information, sharing information with others, how personal information can be access by the data subject and how long information is kept

7 DATA RETENTION AND DELETION

7.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the agreed purposes which shall be documented in the Community Relations Council disposal schedule

8. TRANSFERS

8.1 For the purposes of this clause, transfers of personal data shall mean any sharing of personal data by the Data Receiver with a third party, and shall include, but is not limited to sharing of the Shared Personal Data with any other third party

8.2 The Data Receiver shall share the Shared Personal Data with the Northern Ireland Audit Office, outsourced Internal Audit function, The Executive Office or another statutory body/government agency for the purposes of clause 5.3.

8.3 The Data Receiver shall not share the Shared Personal Data with any other third party without the express written permission of the Data Discloser.

9. SECURITY AND TRAINING

9.1 The Data Discloser shall be responsible for the security of transmission of any Shared Personal Data in transmission to the Data Receiver by using appropriate technical methods.

9.2 The Community Relations Council has appropriate measures in place to protect the Shared Personal Data in their possession against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

- a procedure for processing and security shared personal data received from a funded group
- ensuring IT equipment, including portable equipment is kept in lockable areas when unattended;
- not leaving portable equipment containing the Personal Data unattended;

- ensuring that staff use appropriate secure passwords for logging into systems or databases containing the Personal Data;

- ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;

- limiting access to relevant databases and systems to those of its employee and officers, need to have access to the Personal Data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the Party;

- ensuring all staff handling Personal Data have been made aware of their responsibilities with regards to handling of Personal Data.

9.3 _____ will provide an itemised list of all Shared Personal Information with each transfer of personal information in the format required by the Community Relations Council.

10. DATA SECURITY BREACHES AND REPORTING PROCEDURES

10.1 The Community Relations Council will promptly (and in any event within 24 hours) notify _____ if it (or any of its Processors) suspects or becomes aware of any suspected, actual or threatened occurrence of any Personal Data Breach.

10.2 The Community Relations Council will, where required by Data Protection Law, promptly (and in any event within 72 hours) of becoming aware of the breach notify the breach to the Information Commissioner's Office.

10.3 _____ will, where required by Data Protection Law, notify the Data Subject promptly (and in any event within 72 hours) of being notified of any personal data breach by the Community Relations Council.

10.4 The Parties agree to provide reasonable assistance as is necessary to each other and the Data Subject to facilitate the handling of any Data Security Breach in an expeditious and compliant manner.

11. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE INFORMATION COMMISSIONERS OFFICER

11.1 In the event of a dispute or claim brought by a Data Subject or the Information Commissioner's Office concerning the processing of Shared Personal Data against

either or both Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

11.2 The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner's Office. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

11.3 In respect of breaches relating to this Agreement, each Party shall abide by a decision of a competent court of the Data Discloser's country of establishment or of any binding decision of the relevant Data Protection Authority.

12. WARRANTIES

12.1 Each Party warrants and undertakes that it will:

a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations.

b) Make available to the affected Data Subjects a copy of this Agreement.

c) Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant the Information Commissioner's Office in relation to the Shared Personal Data.

d) Respond to Subject Access Requests in accordance with the terms of this Agreement and in accordance with the Data Protection Law.

e) Take all appropriate steps to ensure compliance with this agreement.

12.2 The Data Discloser warrants and undertakes that it will ensure that the Shared Personal Data are accurate.

13. TERM AND TERMINATION

13.1 The term of this Agreement is that provided for in clause XXXX of in the Letter of Offer *(REFERENCE)* to _____ or to any addendum to that Letter of Offer extending the term.

13.2 The Agreement shall automatically terminate on expiry of the term unless.

13.3 Any such renewal shall be in writing signed by an authorised signatory of both Parties.

14. ROLES AND RESPONSIBILITIES

14.1 Each Party shall nominate a single point of contact within their organisation who can be contacted in respect of queries or complaints regarding Data Protection Law and/or compliance under the terms of this Agreement.

The Community Relations Council	**Funded Group:**
Director of Finance, Administration and Personnel Community Relations Council 2nd Floor Equality House 7-9 Shaftesbury Square Belfast BT2 7DP	

15. THIRD PARTY RIGHTS

15.1 No one other than a Party to this Agreement shall have any right to enforce any of its terms.

16. VARIATION

16.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

17. WAIVER

17.1 No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy,

nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

18. CHANGES TO THE APPLICABLE LAW

18.1 In case the applicable Data Protection Law changes in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that they will negotiate in good faith to review the Agreement in light of the new legislation.

19. NO PARTNERSHIP OR AGENCY

19.1 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party.

19.2 Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

20. ENTIRE AGREEMENT

20.1 This Agreement constitutes the entire agreement between the Parties in relation to the sharing of Student Personal Data.

20.2 Each Party acknowledges that in entering into this Agreement it does not rely on and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.

20.3 Nothing in this clause shall limit or exclude any liability for fraud.

21. FORCE MAJEURE

21.1 Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control. In such circumstances the affected party shall be entitled to a reasonable extension of

the time for performing such obligations. If the period of delay or non-performance continues for 3 months, the Party not affected may terminate this Agreement by giving 30 days' written notice to the affected Party.

22 INDEMNITY

22.1 _____shall indemnify the Community Relations Council and shall keep the Community Relations Council indemnified against all liabilities, losses, damages, costs or expenses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the Community Relations Council arising out of or in connection with any claim made against it in relation to any breach by _____ its employees, agents or processors under Data Protection Law.

23. GOVERNING LAW AND JURISDICTION

23.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of Northern Ireland.

23.2 Each Party irrevocably agrees that the courts of Northern Ireland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

EXECUTED as an agreement:

SIGNED: _____

for and on behalf of ( )

Name:_____ Position:_____

SIGNED:_____

for and on behalf of the COMMUNITY RELATIONS COUNCIL

Name:_____

Position:_____

APPENDIX 9: PRIVACY AGREEMENT FOR EMPLOYEES

The Community Relations Council is committed to protecting the privacy and security of your personal information.

This agreement describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

The Community Relations Council is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.

- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. The following is the purpose or purposes for which we are processing or will process your personal information and the categories of data involved:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and deducting tax and National Insurance contributions.
- Providing information to Northern Ireland Local Government Offices Superannuation Committee (NILGOSC) as required by the Local Government Pension Scheme Regulations (NI) 2014.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.

- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligation.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the working relationship with you.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers. The following activities are carried out by third-party service providers: payroll, HR and Health & Safety Advice and Occupation and IT services.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other public authorities?

We will share your personal information with other public authorities as part of our regular reporting activities on company performance, business development, pay remit reviews or other ongoing operational requirements. In doing so the Community Relations Council will take appropriate steps to pseudonymize your personal data.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the DPO.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the DPO. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where there is something about your particular situation which makes you want to object to processing on this ground. You also

have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer (DPO)

We have appointed a DPO to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Data Protection Officer at (INSERT ADDRESS).

I,_____ (employee/worker/contractor name), acknowledge that on _____ (date), I received a copy of EMPLOYER's Privacy Notice for employees, workers and contractors and that I have read and understood it.

Signature

……

Name

Community Relations Council

GDPR Privacy notice for employees, workers and contractors (UK)

What is the purpose of this document?

The Community Relations Council is committed to protecting the privacy and security of your personal information.

This agreement describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

The Community Relations Council is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.

- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. The following is the purpose or purposes for which we are processing or will process your personal information and the categories of data involved.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and deducting tax and National Insurance contributions.
- Providing information to Northern Ireland Local Government Offices Superannuation Committee (NILGOSC) as required by the Local Government Pension Scheme Regulations (NI) 2014.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To promote the objectives of CRC
- To prevent fraud.

- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information

public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the working relationship with you.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers. The following activities are carried out by third-party service providers: payroll, HR and Health & Safety Advice and Occupation and IT services

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other public authorities?

We will share your personal information with other public authorities as part of our regular reporting activities on company performance, business development, pay remit reviews or other ongoing operational requirements. In doing so the Community Relations Council will take appropriate steps to pseudonymize your personal data.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the DPO.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the DPO. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your

consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer (DPO)

We have appointed a DPO to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Data Protection Officer at:

Gerard McKeown
Director of Finance, Administration and Personnel
Community Relations Council
2nd Floor
Equality House
7-9 Shaftesbury Square
Belfast
BT2 7DP

Telephone: 02890 227500

Fax: 02890 227551

E-mail: gmckeown@nicrc.org.uk

I,_____ (employee/worker/contractor name), acknowledge that on _____ (date), I received a copy of EMPLOYER's Privacy Notice for employees, workers and contractors and that I have read and understood it.

Signature

……

Print Name

……