Data Protection Policy

1. Purpose

This policy defines the data protection responsibilities of the Great British Nuclear (GBE-N) and its employees, contractors and consultants and ensures that all are aware, not only of the requirements of data protection legislation on GBE-N, but also their individual responsibilities in this respect.

This policy also supports compliance with the Data (Use and Access) Act 2025 (DUAA), which governs lawful reuse and access to personal data across public and private sector activities.

2. Scope

This policy applies to all GBE-N employees, contractors and consultants.

3. Policy details

3.1. General

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 provide individuals with rights in relation to personal data held or processed by organisations. These laws also place obligations on organisations to implement appropriate technical and organisational measures to ensure the integrity, confidentiality, and lawful handling of personal information.

GBE-N recognises that Microsoft Teams recordings and transcripts may contain personal data and therefore constitute processing under UK GDPR. Their use must be governed by appropriate organisational controls that define lawful basis, consent requirements, retention periods, and access restrictions.

The Data (Use and Access) Act 2025 (DUAA) introduces further responsibilities for organisations regarding the lawful reuse of personal data, access pathways, and transparency. GBE-N must ensure that any secondary use of personal data such as for internal analytics, regulatory reporting, or public authority access is compatible with the original purpose or otherwise permitted by law and is subject to appropriate governance controls.

GBE-N has a statutory obligation as a Data Controller and, in some cases, a Data Processor, to be accountable for and able to demonstrate compliance with all applicable legislation. Full details of GBE-N's data processing activities, including lawful bases, retention schedules, and data sharing arrangements, are available to staff via the intranet and externally through the organisation's website.

3.2. Responsibilities

The GBE-N Data Protection Officer (DPO) is responsible for ensuring that statutory and regulatory obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA) are met. This includes overseeing the organisation's compliance with data protection principles, lawful reuse of personal data, and access governance under DUAA.

The DPO provides training, guidance, and advice to ensure policy compliance across all GBE-N employees, consultants, and contractors. They are also the designated point of contact for all data protection queries, including subject access requests, objections to data reuse, and concerns regarding data access or sharing.

Directors, Departmental and Functional Heads are responsible for promoting this policy and ensuring its implementation within their respective business units. All GBE-N personnel are expected to incorporate this policy and associated guidance into their daily working practices.

3.3. GDPR Principles

The GDPR provides that six principles be adhered to in the processing of personal data. This is achieved by GBE-N implementing appropriate rules and procedures. All GBE-N employees, contractors and consultants are therefore responsible for ensuring that these rules and procedures are followed. The objectives of the rules and procedures are to ensure that the 6 principles will be complied with, and that all personal data is:

- processed lawfully and fairly and in a transparent manner.
- collected for specified, explicit legitimate purposes and not further processed in a manner incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes.
- accurate and where necessary kept up-to-date.
- kept in a form which permits identification for no longer than is necessary for the specified purpose.
- kept secure subject to appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.

Under the terms of the GDPR, processing of data includes any activity to do with the data involved. All employees or other individuals who have access to, or who utilise, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised third party.

Additionally, in order to comply with the first principle, at least one of the following conditions must also be met.

- the subject has given his/her explicit consent to the processing (such consent must be recorded);
- the processing is necessary for the performance of a contract with the subject;
- processing is required under a legal obligation;
- processing is necessary to protect the vital interests (essential for the life) of the subject or another person;
- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary to pursue the legitimate interests of the Data Controller or third parties (unless it could prejudice the interests of the subject or would constitute processing carried out by a public authority in the performance of their tasks).

3.4. Special category (sensitive) data

Explicit consent of the individual will usually have to be obtained before the data is processed unless the data controller can prove the processing is based on one of the following criteria.

- Compliance with employment law and obligations.
- To protect vital interests (essential for the life) of the data subject.
- The data subject has deliberately made the information public.
- To comply with legal obligations (establishing or defending legal rights).
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Occupational medicine, provision of heath or social care or treatment.
- Public health.
- Scientific or historical research or statistical purposes.

3.5. Data subject access rights

Data subjects have the right to access personal data held about them by GBE-N. This is known as a Subject Access Request (SAR). The process for submitting and responding to SARs is outlined in the Subject Access Request Procedure, which must be followed in all cases.

In addition to access, individuals may exercise other rights under UK GDPR and the Data (Use and Access) Act 2025, including the right to:

- Rectify inaccurate or incomplete personal data.
- Erase personal data where there is no lawful basis for its continued processing.
- Restrict or object to the processing of personal data, including reuse under DUAA.
- Withdraw consent, where processing is based on consent.

All such requests must be referred to the Data Protection Officer (DPO) for assessment and response. The DPO will determine whether the request can be fulfilled in full or in part and will provide a clear justification where any aspect of the request is declined.

Where data reuse is proposed under DUAA, individuals must be informed of the intended purpose and given the opportunity to object, unless the reuse is required by law or justified by public interest.

3.6. Data Privacy Impact Assessments

Data Privacy impact assessments (DPIA's) are a tool that is used to identify and reduce the privacy risks of projects. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

A DPIA will be carried out whenever a “new” project/process involving the use of personal information is being considered/initiated, especially if this involves the use of technology or third-party processors.

A DPIA must also be conducted where data reuse under DUAA introduces new risks or involves access by external parties, regulators, or automated systems.

Signed by

Name	Peter Welch
Position	Corporate Services Director
Signature