North of England Institute of
Mining and Mechanical Engineers

Founded 1852
Royal Charter 1876

NEIMME Data Protection Policy (DPA / GDPR)

Approved by: NEIMME Council **Date: May 2019**

1. Objective

To ensure all personal data handled and held by the Institute are in compliance and in accordance with the Data Protection Act (2018) {DPA} and General Data Protection Regulations {GDPR}.

2. Scope

This Policy refers to safe handling, storage and use of all personal data relevant to the operation of the NEIMME, to include the current and future operations relating to a Young Members Group (YMG) as required under current DPA / GDPR.

NEIMME will make this Policy available to all current and future members of the Institute.

3. Personal Information

Personal information (as defined in legislation) must be handled, recorded, stored and dealt with in a safe and proper manner whether it be on paper or on computer records. As such NEIMME fully adhere to the general principles of the GDPR.

4. The 8 Data Protection Principles

The 8 data protection principles require that personal data shall:

- Be obtained fairly, lawfully and transparent and shall not be processed unless certain conditions are met;
- Be obtained for specific and lawful purposes;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and up to date;
- Not be kept for longer than necessary;
- Be processed in accordance with the data subject's rights;
- Be processed in a manner that ensures appropriate security of personal data which includes protecting against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- Not to be transferred to a country outside of the EU

5. Responsibilities and the Data Protection Officer (DPO)

NEIMME has nominated an existing Council Member as the 'Data Protection Officer' on behalf of the Trustees.

The current DPO is: Steve Martin

6. Obtaining, Disclosing and Sharing Personal Data

Personal data must be collected and stored in a safe manner and must not be disclosed to a third party organisation without prior consent of the individual concerned.

There may be circumstances whereby NEIMME may have a legal duty to disclose personal information in order to ensure certain legal compliance.

Personal contact details may be acquired during the membership application and renewal process whereby the member or potential member duly authorises the 'specific' use of data and for applicable 'contact' purposes (in a lawful manner).

7. Retention, Security and Disposal

Where data is computerised it should be coded, encrypted or password protected.

This secure data should be backed-up regularly and any removable storage media (used as a back-up device) must be kept in a locked storage unit.

Ordinarily personal data should not be kept or transported on lap-tops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on such a device it should be protected by:

- Ensuring data is recorded on such devices only where absolutely necessary;
- Using an encrypted system or stored on separate files with extra protection with higher level passwords;
- Ensuring that laptops or USB drives are not left where they can be stolen or used by unauthorised personnel

Those currently authorised to store and use personal data in this manner are:

Steve Martin, David Bell and Derek Newton

During the period of time whereby NEIMME are operating from remote and private zones due to the 2019 / 2020 refurbishment programme at the Neville Hall in Newcastle-upon-Tyne a limited number of persons have been duly authorised by senior trustees to use such laptops and storage devices in accordance with the aforementioned provisions.

Upon completion of the aforementioned refurbishment programme where NEIMME will then reside and operate as planned from October 2020 the use of personal computers and devices as authorised by the Trustees will be reviewed.

Personal data will be held for no longer than necessary and when required must be disposed of either by destroying data held on paper or / and by deleting all computer and back-up device records.

8. Reporting a Data Security Breach

Any breach noted or identified through whistleblowing Policy should be reported to the DPO who will conduct an investigation and act accordingly subject to the results of the investigation.