

To: The Secretary, ALL BRANCHES AND REGIONAL COUNCILS

Circular No. MF/108/18
Ref: MOM/MEM/DP

30th August 2018

Dear Colleague,

**DATA PROTECTION
European Union General Data Protection Regulations, (GDPR)**

Further to Circular No. MF/60/18, 24th May 2018, the Union's 'IT and Protection of Information Policies and Procedures' were agreed by the National Executive Committee at the June 2018 Statutory Meeting and are enclosed for your reference.

As previously stated, these will represent a minimum standard and will be amended and added to in due course as the Union seeks to provide further supporting guidance across our structures. It is not possible to provide instructions for each individual task that the Union undertakes at this stage, but the enclosed document represents the principles to follow to create an awareness of security. Individuals, whether elected or employed, should therefore review the tasks they undertake and seek to determine the measures they may need to put in place to comply with the requirements of GDPR. The Union's additional guidance in the coming months, which will be subject to the NEC's agreement, will support this process.

There is an onus on the Union and individuals acting on its behalf to ensure compliance. As stated in the enclosed document, the introduction of the Union's new policies and procedures is intended to ensure that the union complies with our legal obligations and the stricter regime we now face. In doing so we also protect the Union, its employees, officials, lay officials and representatives. In the event of a breach of the policies and procedures, the RMT may need to consider measures in accordance with the Union's rules. The Union and individuals may also face legal action. In cases where offences against the law are deemed to have been committed, the Union must report such instances to the appropriate authorities. **Therefore, noting the potential action following a breach, the Union's policies and procedures MUST be adhered to at all times.**

The Union has already experienced a breach following the implementation of GDPR on 25th May 2018 and reported the matter to the Information Commissioner. The breach centred on a membership list being found unattended within an office. Fortunately a member found the list and swiftly returned it to RMT's Head Office. Furthermore, the information within the list was particularly limited, only containing information relevant for its intended purpose. We will continue to work with the ICO to ensure we learn from such instances

and review our processes. Noting this specific example, I would ask all Branch and Regional Council Officials to contact their representatives to ensure that hardcopy documentation is kept on their person or stored securely at all times. Representatives should also be given the opportunity to read the enclosed document. Electronic copies can also be provided on request.

While it is important to read the Policies and Procedures in full, I would draw your specific attention to the following:

Appendix B – Password Advice

This provides guidance to assist with the prevention of unauthorised access to RMT information.

Appendix C – Password Protection Process

This will assist in reducing the risk of unauthorised access to the files you send to those acting on behalf of the Union.

Appendix D – Entitlement to Information

This provides guidance to those in the Union who have a responsibility to handle information/data and ensures that it is not provided to those who are not entitled to receive it.

Data Protection Policy – Branch & Regional Council Officials

Section 3 (page 19) ‘Security of Membership Detail’ states:

- Members, honorary members and Branch/Regional Council officials, (web users) are no different to RMT employees in terms of the provisions of the Data Protection Act in relation to accessing personal data and it is an offence to deliberately access data which they are not entitled to view.
- It is also an offence to reveal members' personal detail to anyone not authorised to access that detail as specified above unless the member(s) has/have given their written permission to do so and it has been authorised by the General Secretary.

Section 4 (pages 19 – 21) ‘Downloading and Receiving Membership Information’ states:

- Information downloaded from Web Membership/eMembership or received from Head Office or a Regional or Shipping Office should not be e-mailed to anyone unless absolutely necessary for organisational purposes and then only to official RMT representatives.
- Reports and lists generated from Web Membership/eMembership or received from Head Office or a Regional or Shipping Office must only be used for official RMT purposes and must never be given to any unauthorised persons or external organisations.
- **WEB USERS MUST NOT PASS CONFIDENTIAL OR SENSITIVE RMT INFORMATION OR ANY MEMBERSHIP DATA TO ANYONE NOT**

ENTITLED TO RECEIVE IT, (remember, membership of a trade union is sensitive information under the Act and must not be revealed to anyone outside of the organisation unless authorised by the General Secretary).

Noting the above it is imperative that those listed within Appendix D, who are entitled to receive specified membership data, do not use it in any way other than for its intended 'organisational' purpose. You must therefore not use the data for any other purpose or send the data to anyone who is not listed within Appendix D, unless authorised by the General Secretary.

To support our lay Branch and Regional Council officials, data protection has been a major element of the eMembership training courses being held at the Bob Crow National Education Centre since 2016. Officials now only have access to records on completion of training and once they have signed a statement to the effect that they understand and accept their responsibilities for protecting sensitive information. The former web resource software has now been switched off to enable the Union to comply with the requirements of legislation and restrict access to those who are trained. We are also in the process of establishing ways and means of including data protection principles and procedures within other relevant courses in the Union's education programme so we can build in as much advice and support as possible.

Yours sincerely,

A handwritten signature in black ink that reads "Mick Cash". The signature is written in a cursive style with a large, sweeping initial 'M'.

Mick Cash
General Secretary