Teachers' Union of Ireland Aontas Múinteoirí Éireann

73 Orwell Road, Rathgar, Dublin 6. D06 YP89
Tel: (01) 4922588 Fax: (01) 4922953
e-mail: tui@tui.ie
website: https://www.tui.ie

1st April 2020

For circulation to branches

Dear Branch Secretary,

Please circulate this advice on General Data Protection Regulation (GDPR) to members in the branch.

General advice on GDPR for members working remotely during the Covid-19 pandemic

During this national emergency period, members and workers in general are directed by the Government (under advice from the National Health Emergency Team) to stay at home to slow the spread of Covid-19 and reduce the risk to family, friends and communities. See official information and guidelines on Covid-19 measures at Gov.ie https://www.gov.ie/en/. The Minister for Education and Skills instructed all schools, colleges and higher education institutes, to close for students until the 29th March 2020. The closure period was recently extended to the 19th April 2020 (for updates see https://www.education.ie/en/). During this period of closures, teachers and lecturers are requested to continue teaching and supporting students where possible, by use of available means from home. Remote working is becoming a new norm during the Covid-19 pandemic emergency. Remote working presents new challenges in terms of maintaining compliance with GDPR. The Data Protection Commissioner has produced a useful summary guide for remote work (see attached PDF or Tiny URL link https://tinyurl.com/tuxgon4).

The following provides members with some general and practical advice on GDPR to assist when working remotely from home.

Permission to use personal data

Get permission from your employer (school/college/ETB/institute/university) to access and use personal data of students and staff for the purposes of remote working. For communications, request access to the email list (and only if necessary, phone number) of students you teach, and other staff as required and if needed. Request external access to the employer's software packages including emails, working documents, communication platforms, virtual learning environments etc. Take time to familiarise yourself with the employer's usage policies regarding software packages. If you are in any doubt about how to use these software packages and data protection issues seek advice and, if required, training from the employer.

Use of Equipment/devices

In the first instance you should request the employer to provide you with the IT and telecommunications equipment necessary to carry out remote work from home. If under the current emergency the employer cannot supply the equipment at this stage, you may decide to request permission to use your own equipment. If you want to use your own equipment seek advice from the employer on whether the equipment is compatible and secure for the purposes of processing student personal data. To protect personal data on devices the following is suggested; install encryption software, use strong passwords and change them regularly, switch on tracking option to enable location finder in case of loss or theft of device, and install up-to-date security software.

Email account

The email account provided by the employer should be used for all work-related matters including; communications with students and other staff colleagues. It is not advisable to use a private personal email account for work purposes. For security of email it is advisable to; change your email password on a regular basis, close the email account when the device is left unattended, do not share your password with others, and update software regularly. It is good practice to clean the email account on a regular basis by deleting emails that have served their purpose. When sending group emails use the BCC option to protect the email addresses of those in the list.

Cybersecurity

Cybercrime is on the increase. Organised crime uses sophisticated methods to defraud and steal; information, identity, data, accounts and funds. To protect data when working remotely online the following should be considered: never provide a requester with your username and password, do not open emails from unknown sources, do not open attachments or URL links from unknown sources and regularly delete emails in the spam and junk folders. Multi-factor authentication is a common way to provide devices and software with an extra security level. Organised crime seeks to target the individual by websites, email and/or phone, and seek to trick you into providing the information they want. Be alert to their schemes. Do not engage with them and report any suspicious activities to the employer or Garda. It is good practice to shut down and switch off power supply to devices when they are not in use. It is advisable to have a password for your home WiFi, this should only be shared with family or trusted guests.

Confidentiality

When working remotely, measures should be taken to secure the confidentiality of work-related data. The following can assist; set a password to log into your device, log out of accounts when leaving the device, password protect documents/folders, advise other users of the device that it contains protected work-related material that should not be accessed. Request other users of the device not to access or download from unsecure websites.

Data breach

If you become aware of a potential data breach (unauthorised access to data, circulation of data to the wrong recipients, loss or thief of data etc.) you should immediately report the matter to the employer, keeping your own record of the time, date and whom you reported the matter to. If you are concerned that your device is hacked, shut it down, turn off the power supply and seek immediate advice from your employer.

Data access request

An individual has a right to request an organisation to; disclose what type of personal data (if any) is stored relating to the individual and to supply copies of the personal data (if requested). Devices used for remote working are subject to data access requests. Data access requests are managed by the employer, who will circulate the data access request to the relevant staff and detail the instructions to be followed. If a member receives a data access request from an individual, the request should be sent immediately to the employer for processing.

It is advisable to get familiar with the employer's policy on data protection and any new measures introduced to accommodate remote working from home. In circumstances where the employer has not issued guidelines to staff, then the Data Protection Commission's guidelines should be followed.

I trust this information is of assistance, please send any GDPR queries to dpo@tui.ie .

Regards,

Dr. Aidan Kenny
Data Protection Officer