XPS Pensions Group

Response to COVID-19 pandemic update – November 2020

From the outset of the COVID 19 pandemic, our top priority has been ensuring the health and safety of our employees whilst continuing to provide a high level of service to our clients and also recognising the increase in cyber threats due to changes in how we work.

COVID -19 has made a significant impact on all our lives, including how and where we work. These changes resulted in a shift in the XPS Group operating model, with all staff now able to work from home. In order to achieve this some processes needed to be re-engineered to ensure they worked effectively under this new model and upgrades were required to some IT systems to make this happen.

A key focus for management throughout this time has been the physical and mental wellbeing of our staff and we have put in place a number of initiatives, keeping people connected formally and informally, providing a variety of online support and training relating to mental health etc.

Senior Management continue to provide weekly updates to the Group providing reassurance and encouragement as well as reminders regarding current cyber threats. This is backed up by an annual cyber threat training programme.

The security of the data we process on behalf of clients continues to be of paramount importance. All pre COVID-19 policies and controls that protect our systems and data remain in place and all staff are required to fully comply with them. We have also put in place several additional measures to help protect the security of client data during this time:

1. Staff continue to be reminded of the key requirements that they need to follow whilst in a home environment:
   - Client or company information is not to be shared with family or household members.
   - Screens must be locked when stepping away from the device.
   - Staff are not permitted to download any software to corporate devices. Specific software requirements must be raised via IT.
   - No client or company information is permitted to be saved onto own devices i.e. mobile phones or computers.
   - Laptops must be fully shut down when staff have finished their work for the day.
   - Laptops and papers must be stored securely at home when not being used.
   - All confidential documents must be returned to the office, when possible, to be destroyed securely.

2. A project to provide all staff with Company issued laptops has been completed. This has removed the interim dependency of some staff using personal devices to access resources through a fully secured and controlled route.
3. We have extended our use of Multi Factor Authentication (MFA).
4. Additional mandatory cyber training focused on the increased threat of phishing has been rolled out.
5. Advance Threat Protection (ATP) has been introduced which uses a virtual environment to check attachments in email messages before delivery to recipients.
6. The introduction of password vaults to enable secure storage of passwords.
7. We reminded all staff of the guidance available in the Group policies, including the fact that suspected incident reporting processes remain unchanged.
8. Physical security risk assessments have been carried out recognising that offices may not be occupied at usual levels, and ensuring our offices are following COVID 19 safe measures as laid out in the relevant guidance.
9. We expanded the use of existing approved suppliers to enable remote printing for all mail.
10. We have also updated our starter and leaver process to reflect current working environments.

Our Business Continuity Plans have been updated to reflect the changes made during the pandemic which will allow us to re-apply our working from home strategy, at short notice in the future, should we need to.