Data Protection Impact Assessment (DPIA) Summary

DPIA019 REF - Stage 2 Summary
Date Reviewed: 01/07/2024
Service Area/Team: Digital Services
Project name/title for work: Microsoft 365 Cloud Migration
SUMMARY OF PROJECT: Humberside Fire and Rescue Service use Microsoft 365. It is a tool that allows staff to access emails and personal documents anywhere with their own username and password. The username is assigned to them when they start working for HFRS. This will improve accessibility for staff as long as they have internet access. Sharing documents and information has also been made easier with Microsoft365. We require staff names and e-mail addresses to connect them to the Microsoft 365 environment.
Assurances: • Only people with Humberside fire and rescue Microsoft 365 accounts can access documents. • Users can only delete records in their own folders. There is a record of all activity that happens in the software. • The system administrator has a tight control over who has access to the system. The login is controlled through the main network so the moment someone leaves, they cannot access the system. • Staff must complete data protection training • The system records all activity that takes place. • We train staff on how to recognise a request for information, rectification or erasure. • M365 can block any device or IP address that might cause a security risk or breach. • If a colleague uploads a document, it is scanned before going onto the cloud platform. • Colleagues cannot access any internal systems or use the VPN on personal devices. • Staff should change their passwords every 90 days. • If a laptop is stolen, we can block this device as well as remove it from the domain and stop this from being logged into. Our tablet devices can also be blocked straight away if lost or stolen. We are also able to track devices. • Machines have a screen saver initiated after 5 minutes of no activity. We also have a policy that states users are not to leave their devices unattended without locking them. • After 30 days if a device hasn't been on the domain or connected to the Anti-Virus software, it will be temporarily blocked from accessing the network. This is until the person who has the device contacts digital services.