



Information security is a way of life at UKIM. Our established policy framework is certified to the highest possible standard and has been adapted to ensure compliance with the new EU General Data Protection Regulation (GDPR).

**1 DATA PROTECTION BY DESIGN**



We have an established change management function that ensures we manage our obligations under **GDPR...**



**THROUGHOUT THE LIFECYCLE OF ANY BUSINESS CHANGE.**

**2 NEAR MISS REPORTING**



Our robust procedure for near miss detection, investigation and internal reporting is followed right across our business.



THIS COLLECTIVE RESPONSIBILITY KEEPS OUR **INFORMATION SECURE.**

**4 ASSET MANAGEMENT**



We have strict controls in place to manage our processes with information audits and process registers forming a key part of our Information Security Management System. **All data processing activities are systematically logged, along with the nature of the data and its lifecycle.**

**3 SUPPLIER MANAGEMENT**



Where suppliers access, store, process or transfer data on our behalf our Supplier Management Policy instils a due diligence process which includes supplier assessment, onboarding and review.

**5 POLICY FRAMEWORK**

**100+**



Our established policy framework, combined with our culture of compliance, secures a protective seal around the hundreds of pieces of personal sensitive data we process every day.

**6 AUTHORITY TO PROCESS**



We recognise the importance of giving individuals choice and control and have always sought authority to process personal data.



WE WILL CONTINUE TO **ENSURE THAT OUR CONTROLS ARE GDPR COMPLIANT.**

**8 THE RIGHTS OF INDIVIDUALS**

We understand our obligations to data subjects in regards to their rights to privacy. All stored data is encrypted and is subject to our retention policy. We have procedures in place to manage any requests for...



DATA ANONYMISATION



RESTRICTION



ERASURE



RECTIFICATION

**7 SUBJECT ACCESS REQUESTS**



We have an established protocol for responding to requests from our data subjects and these are managed within our case management system to track progression and adherence.

**9 PRIVACY INFORMATION**



Trust and transparency are key elements of **GDPR**. We respect that individuals have the right to be informed about the collection and use of their data and we have set out clear guidance on how data is processed in our Fair Processing Notice.

**10 GOVERNANCE & ACCOUNTABILITY**

Our commitment to data security is guided by a network of components, including our ISO27001 certified data management system, an Information Security Committee, Data Security Champions, Data Protection Representatives, a Data Protection Officer and Caldicott Guardian – all with a key focus on supporting adherence to the highest possible standards for handling data.