**Personal Identifiable Data Information Asset Register**

**Guidelines**

1. **Background**

Information Asset Owners (IAO) are responsible for all information assets within their area of responsibility. These guidelines are for assisting IAOs and users in the identification and registration of their information assets which contain Personal Identifiable Data (PID).

PID is data relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as:

* name,
* an identification number,
* location data,
* an online identifier

or to one or more factors specific to the:

* physical,
* physiological,
* genetic,
* mental,
* economic,
* cultural or
* social identity;

Sensitive or special category personal data is personal data consisting of information as to:

* race;
* ethnic origin;
* politics;
* religion;
* membership of a trade union;
* health;
* sex life;
* sexual orientation;
* genetics;
* biometrics (where used for ID purposes)

1. **Guidance**

The Personal Identifiable Data Information Asset Register (PIDIAR) has been developed to capture those assets containing personal data that have not been captured in the Systems Information Asset Register (SIAR). The SIAR, which sits alongside the PIDIAR, contains all corporate systems used within the university and identified in the University Information Systems Catalogue. Therefore, any PID residing in a system identified in the SIAR does not need to be captured as these systems are all have IT managed back-up processes.

Systems identified in the SIAR:

* Secure Central File Stores – in-house secure working and H drives. (not C drives).
* Data Safe Haven
* Tribal SITS Student Administration System
* Unit 4 Agresso Finance System
* Midland HR
* G4S Security Access Control System
* Razors Edge Alumni Management
* Alma Library management
* Canvas Virtual Learning
* Current Research Information Services
* OCCAM Accommodation System
* Scientia Syllabus +
* Telepen
* Bibliotheca
* Preservica
* SORA
* MS 365 (Teams, SharePoint, OneDrive, Outlook)
* REDCap

Examples of assets which need to be captured in the PIDIAR are:

* Data stored directly on a SGUL laptop or PC (C Drive, Desktop) and not into a file store.
* Data stored on a SGUL procured device which is not managed by SGUL IT. e.g. Apple Macs, storage devices and will not have an IT Services reference number tab.
* Data stored on a personal device and not registered with SGUL IT.
* Data stored on a cloud-based application which is not supported by SGUL IT.
* Hard copy stores – filing cabinets etc

The PIDIAR spreadsheet columns are self-explanatory with further guidance provided in row 3 of the spreadsheet. Any questions regarding completion of the PIDIAR should be referred to your Information Governance Lead or the Head of Information Governance.

PIDIAR entries are to be reviewed annually by the IAOs or when an asset has been added or removed.