Introduction

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organisation sets about fulfilling its mission.

In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organisation, from values through to actions and results.

Depending on the organisation, principles may be established within different domains and at different levels. Two key domains inform the development and utilisation of architecture:

- **Enterprise** principles provide a basis for decision-making throughout an organisation, and inform how the organisation sets about fulfilling its mission. Such principles are commonly found as a means of harmonising decision-making across an organisation. In particular, they are a key element in a successful architecture governance strategy.

  Within the broad domain of enterprise principles, it is common to have subsidiary principles within a business or organisational unit. Examples include ICT, HR, frontline policing & protective services arenas. These principles provide a basis for decision-making within the subsidiary domain and will inform architecture development within the domain.

- **Architecture** principles are a set of principles that relate to architecture work. They reflect a level of consensus across the organisation, and embody the spirit and thinking of existing enterprise principles. Architecture principles govern the architecture process, affecting the development, maintenance, and use of the enterprise architecture.

Architecture principles may restate other organisational guidance in terms and form that effectively guide architecture development.

Characteristics of Architecture Principles

Architecture principles define the underlying general rules and guidelines for the use and deployment of all ICT capabilities across the organisation. They reflect a level of consensus among the various elements of the organisation, and form the basis for making future ICT decisions.

Architecture Principles

Business Principles

Principle 1: Primacy of Principles

Statement: These principles of information management apply to all areas within the organisation.

Rationale: The only way we can provide a consistent and measurable level of quality information to decision-makers is if all areas abide by the principles.

Implications: Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information.

> Information management initiatives will not begin until they are examined for compliance with the principles.
>
> A conflict with a principle will be resolved by changing the framework of the initiative.

Principle 2: Maximise Benefit to Policing

Statement: Information management decisions are made to provide maximum benefit to the organisation as a whole.

Rationale: This principle embodies "service above self". Decisions made from an organisation-wide perspective have greater long-term value than decisions made from any particular organisational perspective. Maximum return on investment requires information management decisions to adhere to organisation-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.

Implications: Achieving maximum organisation-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change.

Application development priorities must be established by the entire organisation for the entire organisation.

Applications components should be shared across organisational boundaries.

Information management initiatives should be conducted in accordance with the organisation and national plan. Individual areas should pursue information management initiatives which conform to the blueprints and priorities established by Information Management Department. We will change the plan as we need to.

As needs arise, priorities must be adjusted. A forum with comprehensive organisation representation should make these decisions.

Principle 3: Information Management is Everybody's Business

Statement: All areas of the organisation are accountable for the information management decisions defined and enforced by the Information Management Department and National guidelines.

Rationale: Information users are the key stakeholders, or customers, in the application of technology to address a business need. In order to ensure information management is aligned with the business, all areas of the organisation must be involved in all aspects of the information environment. The business experts from across the organisation and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of ICT.

Implications: To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment.

Commitment of resources will be required to implement this principle.

Principle 4: Business Continuity

Statement: Organisational operations are maintained in spite of system interruptions.

Rationale: As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the organisation must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop organisational activities. Areas of the organisation must be capable of operating on alternative information delivery mechanisms.

Implications: Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities.

Recoverability, redundancy, and maintainability should be addressed at the time of design.

Applications must be assessed for criticality and impact on the organisation mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

Principle 5: Common Use Applications

Statement: Development of applications used nationally, regionally or the organisation as a whole is preferred over the development of similar or duplicative applications which are only used by a subset of users within the organisation.

Rationale: Duplicative capability is expensive and proliferates conflicting data.

Implications: Areas that depend on a capability which does not serve the entire organisation must change over to the replacement single capability. This will require establishment of and adherence to a policy requiring this.

Areas will not be allowed to develop capabilities for their own use which are similar/duplicative of organisation-wide or regional capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.

Data and information used to support organisational decision-making will be standardised to a much greater extent than previously. This is because the smaller, area capabilities which produced different data (which was not shared among other areas) will be replaced by organisation-wide, regional or national capabilities. The impetus for adding to the set of these shared capabilities may well come from an area making a convincing case for the value of the data/information previously produced, but the resulting capability will become part of the single system, and the data it produces will be shared across the constabularies as a whole, regionally or nationally.

Principle 6: Service Orientation

Statement: The architecture is based on a design of services which mirror real-world business activities comprising the organisational (or discreet areas of) business processes.

Rationale: Service orientation delivers organisational agility and Boundary-less Information Flow.

Implications: Service representation utilises business descriptions to provide context (i.e., business process, goal, rule, policy, service interface, and service component) and implements services using service orchestration.

Service orientation places unique requirements on the infrastructure, and implementations should use open standards to realise interoperability and location transparency.

Implementations are environment-specific; they are constrained or enabled by context and must be described within that context.

Strong governance of service representation and implementation is required.

A “Litmus Test”, which determines a “good service”, is required.

Principle 7: Compliance with Law

Statement: Organisation information management processes comply with all relevant laws, policies, and regulations.

Rationale: Organisation policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

Implications: The organisation must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data.

Education and access to the rules. Efficiency, need, and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications.

Principle 8: ICT Responsibility

Statement: The ICT function is responsible for owning and implementing ICT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

Rationale: Effectively align expectations with capabilities and costs so that all projects are cost-effective. Efficient and effective solutions have reasonable costs and clear benefits.

Implications: A process must be created to prioritise projects.

The ICT function must define processes to manage business unit expectations.

Data, application, and technology models must be created to enable integrated quality solutions and to maximise results.

Principle 9: Protection of Intellectual Property

Statement: The organisation's Intellectual Property (IP) must be protected. This protection must be reflected in the ICT architecture, implementation, and governance processes.

Rationale: A major part of an organisation's IP is hosted in the ICT domain.

Implications: While protection of IP assets is everybody's business, much of the actual protection is implemented in the ICT domain. Even trust in non-ICT processes can be managed by ICT processes (email, mandatory notes, etc.).

A security policy, governing human and ICT actors, will be required that can substantially improve protection of IP. This must be capable of both avoiding compromises and reducing liabilities.

Principle 10: Regional & National Delivery in mind

Statement: Solutions should be designed with the aspirational capability of delivering a national solution although in the interim an expectation of utilisation across a region.

Rationale: To ensure easy adoption of force designed solutions the ability to either extend the scale of the application or to allow additional instances to deliver regional or a national capability should be considered during the design phase.

Implications: All forces within the UK are tasked with performing the same tasks. Traditionally each force has defined what technology is to be used to achieve a specific capability. To meet the funding targets and to improve inter-force information sharing forces need to standardise on the applications used.

When designing a new solution, the design must take into account how it could be re-used to deliver a capability to x-forces without the need to redesign the underlying platform. This principle will result in a reduction in disparate systems used, improve data sharing while reducing implementation and operating costs.

Principle 11: Requirements-Based Change

Statement: Only in response to business needs and demand are changes to applications and technology made.

Rationale: This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to ICT changes. This is to ensure that the purpose of the information support — the transaction of business — is the basis for any proposed change. Unintended effects on business due to ICT changes will be minimised. A change in technology may provide an opportunity to enhance the business process and, hence, change business needs.

Implications: Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.

We don't fund a technical improvement or system development unless a documented business need exists.

Change management processes conforming to this principle will be developed and implemented.

This principle may bump up against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. The purpose of this principle is to keep us focused on business, not technology needs responsive change is also a business need. As an enabling service, IT should work with the business to ensure the end to end impact has been envisaged.

Principle 12: Responsive Change Management

Statement: Changes to the organisational information environment are implemented in a timely manner.

Rationale: If people are to be expected to work within the organisational information environment, that information environment must be responsive to their needs.

Implications: IT have to develop processes for managing and implementing change that do not create delays.

An organisation who feels a need for change will need to connect with appropriate governance channels to facilitate explanation and implementation of that need.

If IT are going to make changes, they must keep the architectures updated.

Dependent on volume, this principle could have a reasonable resource demand.

This will conflict with other principles (e.g., maximum organisation-wide benefit, organisation-wide applications, etc.).

Technology Principles

Principle 13: Cloud First

Statement: The suitability of hosting applications & services in the cloud should be given for all requirements in accordance with national guidance.

Rationale: To deliver solutions that can be scaled to provide a capability to x-forces cloud services should be considered as the hosting platform.

Services such as Software as a Service (SaaS), Platform as a Services (PaaS) and Infrastructure as a Service (IaaS) should be considered above local or collaborative implementations where applicable to ensure services can develop and evolve.

Implications: Cloud hosted Software as a Services, in their very design, can be simply scaled as demand requires.

If PaaS or IaaS are selected, then the services hosted must be designed to fully utilise the capabilities of this platform, including scaling and authentication.

A standardised cloud platform must be defined to ensure all solutions sit within the same environment and the linking of data must be defined where applicable.

Principle 14: Control Technical Diversity

Statement: Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments. When looking at the introduction of new technology – it should where possible be considered as a replacement for an existing environment rather than additive if possible

Rationale: There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained.

Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the organisation brings the benefits of economies of scale. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technologies.

Implications: Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.

Technology choices will be constrained by the choices available within the technology standards. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place.

We should not be freezing technology baseline. Embrace technology advances and change the technology standards when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

The 80/20 rule needs to be applied. If an existing capability delivers 80% of the required functionality this must be the chosen platform unless this poses a significant organisational risk, or is unable to meet a national requirement.

Principle 15: Interoperability

Statement: Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

Rationale: Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing ICT investments, thus maximising return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.

Implications: Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.

A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.

The existing ICT platforms must be identified and documented.

Data Principals

Principle 16: Data is an Asset

Statement: Data is an asset that has value to the organisation and is managed accordingly.

Rationale: Policing is an information-led activity, and information assurance is fundamental to how the police service manages many of the challenges faced in policing today. It is vital for maintaining public confidence and for the efficient, effective, safe and secure conduct of operations and services. Without robust information assurance governance and processes, there is a significant risk of compromise, potentially leading to the facilitation of crime, public safety issues, hindrance to investigations, financial loss, damage to organisational reputation and, consequently, a reduction in confidence from the public and partners.

Implications: This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all areas within the organisation understand the relationship between value of data, sharing of data, and accessibility to data.

Information Asset Owners (IAO) must have the authority and means to manage the data for which they are accountable in line with MOPI.

Nationally we must make the cultural transition from “data ownership” thinking to “data stewardship” thinking especially as we look to transition more services and storage to flexible architectures such as “the cloud”.

The role of the IAO is critical because obsolete, incorrect, or inconsistent data could be passed to personnel and adversely affect decisions across the organisation.

Part of the role of IAO, who manages the data, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality

— it is probable that policy and procedures will need to be developed for this as well.

A forum with comprehensive organisation-wide representation should decide on process changes suggested by the steward.

Since data is an asset of value to the entire organisation, data stewards accountable for properly managing the data must be assigned at the organisation level.

Principle 17: Data is Shared

Statement: Users have access to the data necessary to perform their duties; therefore, data is shared, where appropriate, across the country and were applicable with partner agencies.

Rationale: Timely access to accurate data is essential to improving the quality and efficiency of decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The organisations hold a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability and appetite of the organisations to efficiently share these islands of data.

Shared data will result in improved intelligence, decisions etc. since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

Implications: This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all areas within the organisation understand the relationship between value of data, sharing of data, and accessibility to data.

To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term.

For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment.

We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible.

For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.

For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the organisation.

Data sharing will require a significant cultural change.

This principle of data sharing will continually "bump up against" the principle of data security. Under no circumstances will the data sharing principle cause confidential data to be compromised, however we must ensure that the need to know continues to apply, we must ensure are data assets continue protect those under threat, harm etc and assist in the investigation of crime.

Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the organisation-wide "virtual single source" of data.

Principle 18: Data is Accessible

Statement: Data is accessible for users to perform their functions.

Rationale: Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an organisation perspective to allow access by a wide variety of users. Staff/officer time is saved and consistency of data is improved.

Implications: This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all areas within the organisation understand the relationship between value of data, sharing of data, and accessibility to data.

Accessibility involves the ease with which users obtain information.

The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of organisation users and their corresponding methods of access.

Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.

Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require a large cultural shift with an education process and a change in the national risk appetite, which currently supports a belief in “ownership” of data by functional units inside the organisations.

Principle 19: Information Asset Owner

Statement: Each data element has a Information Asset Owner accountable for data quality.

Rationale: One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the organisation. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the Information Asset Owner makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the Information Asset Owner will have sole responsibility for data entry which eliminates redundant human effort and data storage resources.

Implications: Real trusteeship dissolves the data “ownership” issues and allows the data to be available to meet all users’ needs. This implies that a cultural change from data “ownership” to data “trusteeship” may be required.

The Information Asset Owner will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.

It is essential that the Information Asset Owner has the ability to provide user confidence in the data based upon attributes such as “data source”.

It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee.

Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.

As a result of sharing data across the organisation, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognise the importance of this trusteeship responsibility.

Principle 20: Common Vocabulary and Data Definitions

Statement: Data is defined consistently throughout the organisation, and the definitions are understandable and available to all users. If national standards exist these must be applied to ensure local alignment.

Rationale: The data that will be used in the development of applications must have a common definition throughout, to enable sharing of data. A common vocabulary will facilitate communications and enable dialog to be effective. In addition, it is required to interface systems and exchange data.

Implications: We are lulled into thinking that this issue is adequately addressed because there are people with "data administration" job titles and forums with charters implying responsibility. Significant additional energy and resources must be committed to this task. It is key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community — this is more like a common vocabulary and definition.

The ICT department must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the organisation.

Whenever a new data definition is required, the definition effort will be co-ordinated and reconciled with the organisation "glossary" of data descriptions. A data administrator will provide this coordination.

Ambiguities resulting from multiple parochial definitions of data must give way to accepted organisation-wide definitions and understanding.

Multiple data standardisation initiatives need to be co-ordinated.

Functional data administration responsibilities must be assigned.

Principle 21: Data Security

Statement: Data is protected from unauthorised use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, restricted and confidential information.

Rationale: Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorised for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

Implications: Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control. Data owners and/or functional users and Information Management and if relevant, the National Accreditor, must determine whether the aggregation results in an increased classification level. We will need appropriate policy and procedures to handle this review and declassification. Access to information based on a need-to-know policy will force regular reviews of the body of information.

The current practice of having separate systems to contain different classifications needs to be rethought. Is there a software solution to separating classified and unclassified data? The current hardware solution is unwieldy, inefficient, and costly. It is more expensive to manage unclassified data on a classified system. Currently, the only way to combine the two is to place the unclassified data on the classified system, where it must remain.

In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level. This will require challenging the current information marking policy & controls required centrally.

Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labelling for access to pre-decisional, restricted and confidential information must be determined.

Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation. Organisational information must be safeguarded against inadvertent or unauthorised alteration, sabotage, disaster, or disclosure.

Data needs to be managed in line with the Management of Police Information (MOPI) standards.

Principle 22: Management of Police Information (MoPI)

Statement: Data must be managed in accordance with MoPI guidelines.

Rationale: The principle of management of police information (MoPI) provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information.

Implications: If the requirements of MoPI are not considered at the design phase of any new solution, the application of the MoPI rules will be complex to retrofit.

Any data design must take into Consideration how data is to be classified ensuring RRD rules can be effectively applied.

Principle 23: Master Data Management

Statement: There should only be a single master working copy of data held.

Rationale: Application designs will deliver a single instance of data. This will improve information governance and deliver opportunities for the linking of data from multiple applications while maintaining data integrity.

In addition, the cost of hosting and managing multiple copies will be removed.

Implications: Multiple copies of data is complex to manage and costly to store. Solutions should be designed in such a way as to remove the need for multiple copies of data to achieve a variety of functions.

The underlying data store must be designed in such a way that it can be extended to deliver future requirements.

Application Principles

Principle 24: Technology Independence

Statement: Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.

Rationale: Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves.

Realising that every decision made with respect to ICT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software.

Implications: This principle will require standards which support portability.

For Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications, there may be limited current choices, as many of these applications are technology and platform-dependent.

Subsystem interfaces will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the enterprise architecture.

Middleware should be used to decouple applications from specific software solutions.

As an example, this principle could lead to use of Java, and future Java like protocols, which give a high degree of priority to platform independence.

Principle 25: Ease-of-Use

Statement: Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.

Rationale: The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the organisation's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low.

Using an application should be as intuitive as driving a different car.

Implications: Applications will be required to have a common "look-and-feel" and support ergonomic requirements. Hence, the common look-and-feel standard must be designed and usability test criteria must be developed.

Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.

Principle 26: Single Authentication Model

Statement: All user authentication will be delivered from a single central user directory. This model will be applied locally\regionally and federated centrally.

Rationale: To simplify the user experience, while improving security, all applications will be required to authenticate access using a central access directory, and not require any credentials to be provided by the user.

For cloud or hosted solutions, the authentication platform should be federated to the local force directory allowing administration to occur locally using the existing tools and processes.

NOTE: If a national IAM solution is delivered all cloud and hosted applications must utilise this platform to perform user authentication.

It is also advised that this directory should be linked to the force HR system to ensure staff information is up to date.

Implications: Simplifying the logon process improves productivity, while improving security. Users who have multiple logon credentials are more likely to write them down introducing security risks. In addition, many applications that hold local user information do not enforce password policies which result in passwords remaining unchanged for long periods.

By standardising on a single authentication platform, application access can be delivered and managed centrally. This will allow ICT staff to manage the granting and revocation of access rights using existing and familiar tools.

In addition to improved security and a simple user process, this will also allow data to be shared between applications while maintaining users are only able to access the information they have been granted the specific rights to in the source application.