APPENDIX 1B

New Forest
DISTRICT COUNCIL

ICT STRATEGY 2018-2022

Appendix B – Principles for ICT Architectural Decisions

Introduction

These principles have been adapted from TOGAF Enterprise Architecture to provide a set of guiding rules for how ICT decisions are made at NFDC. These principles are aimed at ensuring that consistent decisions are made that protect the integrity of the ICT architecture and the value of the investment in ICT at NFDC.

Each principle is structured in the same way to provide clarity of the purpose, scope, rationale and implications of the principle. They are grouped into four categories of business, data, applications and technology.

Appendix B – Principles for ICT Architectural Decisions

Business Principles

Principle 1:

ICT Responsibility

Statement:

The ICT organization is responsible for owning and implementing IT 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 prioritize projects.

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

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

Principle 2:

Maximize Benefit to the Council

Statement:

Information management decisions are made to provide maximum benefit to the Council as a whole.

Rationale:

This principle embodies "service above self". Decisions made from a Council-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information management decisions to adhere to Council-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 Council-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change.

Some services may have to concede their own preferences for the greater benefit of the entire Council.

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

Applications components should be shared across organizational boundaries.

Information management initiatives should be conducted in accordance with the Council plan. Individual services should pursue information management initiatives which conform to the blueprints and priorities established by the Council. We will change the plan as we need to. As needs arise, priorities must be adjusted. These decisions will be made via agreed governance bodies.

Principle 3:

Business Continuity

Statement:

Council operations are maintained in spite of system interruptions.

Rationale:

Appendix B – Principles for ICT Architectural Decisions

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 Council 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 Council activities. The Council business functions 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 assure 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 Council mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

Principle 4:

Compliance with Law

Statement:

Council information management processes comply with all relevant laws, policies, and regulations.

Rationale:

Council 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 Council 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.

Appendix B – Principles for ICT Architectural Decisions

Data Principles

Principle 5:

Data is an Asset

Statement:

Data is an asset that has value to the Council and is managed accordingly.

Rationale:

Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

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 services within the Council understand the relationship between value of data, sharing of data, and accessibility to data.
Stewards must have the authority and means to manage the data for which they are accountable.
We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking.
The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to Council personnel and adversely affect decisions across the Council. It could also have GDPR consequences.
Part of the role of data steward, 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.
Since data is an asset of value to the entire Council, data stewards accountable for properly managing the data must be assigned at the Council level.

Principle 6:

Data is Shared

Statement:

Users have access to the data necessary to perform their duties; therefore, data is shared across Council functions and services.

Rationale:

Timely access to accurate data is essential to improving the quality and efficiency of Council 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 Council holds 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 of the organization to efficiently share these islands of data across the organization.

Shared data will result in improved decisions 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:

Appendix B – Principles for ICT Architectural Decisions

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 Council.
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.
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 Council-wide "virtual single source" of data.

Principle 7:

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 Council perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.

Implications:

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 Council 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 an education process and a change in the organizational culture, which currently supports a belief in "ownership" of data by functional units.

Principle 8:

Data Trustee

Statement:

Each data element has a trustee 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 Council. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times,

Appendix B – Principles for ICT Architectural Decisions

the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources.

Note:

A trustee is different than a steward - a trustee is responsible for accuracy and currency of the data, while responsibilities of a steward may be broader and include data standardization and definition tasks.

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

It is essential that the trustee 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 Council, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility.

Principle 9:

Common Vocabulary and Data Definitions

Statement:

Data is defined consistently throughout the Council, and the definitions are understandable and available to all users.

Rationale:

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

Implications:

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

Whenever a new data definition is required, the definition effort will be co-ordinated and reconciled with the corporate "glossary" of data descriptions. The Council data administrator will provide this co-ordination.

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

Multiple data standardization initiatives need to be co-ordinated.

Functional data administration responsibilities must be assigned.

Principle 10:

Data Security

Statement:

Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.

Appendix B – Principles for ICT Architectural Decisions

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. GDPR is key here.

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 must determine whether the aggregation results in an increased classification level. We will need appropriate policy and procedures to handle this review and de-classification. 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.

Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labeling for access to pre-decisional, decisional, classified, sensitive, or proprietary 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 unauthorized access and manipulation. Headquarters information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

Need new policies on managing duration of protection for pre-decisional information and other works-in-progress, in consideration of content freshness.

Appendix B – Principles for ICT Architectural Decisions

Application Principles

Principle 11:

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.

Realizing that every decision made with respect to IT 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.
Application Program Interfaces (APIs) will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the Council 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 12:

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 Council'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.

Appendix B – Principles for ICT Architectural Decisions

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 13:

Best FIT Applications

Statement:

Implementation of common 'out of the box' applications, with only minimal user configuration, is preferred over the development of custom applications.

Rationale:

Customisation is expensive to develop and prohibitive to maintain and upgrade. It inhibits changes to working practices and stifles new best practice coming into the Council.

Implications:

Services will not be allowed to procure or develop customised applications. We will move to more and more standard packaged applications running either on public cloud or our own servers. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced. It will reduce ongoing costs for maintenance and upgrade and standardise the way the Council works in line with best practice.

Appendix B – Principles for ICT Architectural Decisions

Technology Principles

Principle 13:

Requirements-Based Change

Statement:

Only in response to business needs 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 IT 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 IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.

Implications:

Changes in implementation will follow full examination of the proposed changes using the Council 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.

Principle 14:

Responsive Change Management

Statement:

Changes to the Council information environment are implemented in a timely manner.

Rationale:

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

Implications:

We have to develop processes for managing and implementing change that do not create delays.

A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.

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

Adopting this principle might require additional resources.

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

Principle 15:

Control Technical Diversity

Statement:

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale:

Appendix B – Principles for ICT Architectural Decisions

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 Council brings the benefits of economies of scale to the Council. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

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 blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
We are not freezing our technology baseline. We welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

Principle 16:
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 IT investments, thus maximizing 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 IT platforms must be identified and documented.