YORKSHIRE DALES NATIONAL PARK AUTHORITY **Item 5**

Meeting: **FINANCE AND RESOURCES**
Date: **6 December 2022**

Report: **IT STRATEGY 2023 - 2028**

Purpose of the report

1. For Members to review and approve the Information Technology (IT) Strategy 2023 – 2028.

Recommendation

2. Members are asked to approve the draft IT Strategy.

Strategic Planning Framework

3. The information and recommendation contained in this report are consistent with the Authority's statutory purposes and its approved strategic planning framework, and specifically Action Plan Objective 38, '*Provide facilities and IT systems that are fit for purpose and support the effective delivery of our services'*, and Action 38.4, '*Review and revise the 5-year IT Strategy'*.

Background

4. The pace of change in IT since the last edition of this Strategy (2016) has showed no signs of slowing; areas of particular interest include virtualised cloud environments, increased remote working, site working, collaboration capabilities, video conferencing, and moving to Microsoft 365 (MS365) and associated inclusive products. When a system or its contract comes up for fundamental review, we will look at the best ways of providing those services in the light of any new technologies available. Such opportunities could include joint purchasing arrangements with other National Park Authorities or Local Authorities.

5. The detailed Strategy setting out how we plan to manage and develop the Authority's IT systems over the next 5 years is attached to this report as an **Annex**. The overall purpose of this Strategy is to ensure that the systems we operate remain fit for purpose, and are developed in such a way that supports the work of the Authority.

6. The activities needed to manage our IT systems and assets comprise capital works (development work; equipment purchase, both hardware and software),

and more routine systems-management activity. A detailed budget has been prepared in support of the strategy presented here, timetabling the work to be undertaken over the period with best estimates of costs. It is not included in the strategy but is available to Members on request. Expenditure falls into two categories:

- Capital works of £349k, to be funded by an earmarked IT Reserve. Note that these are the total costs for the 5-year period covered by the Strategy.

- Annual routine licencing, maintenance and support costs estimated at £168k in 2023/24 increasing by 2.2% thereafter, are included within the Authority's annual revenue budgets.

7. The developments proposed within the Strategy will secure the Authority's data and IT equipment while working outside the corporate IT network, while also providing enhanced data governance and management information. Improved mobile connectivity and communications systems are planned, to enable staff to remain in contact and work collaboratively whilst working remotely. The infrastructure works proposed within the Strategy provide continued resilience of the on-site IT systems.

Conclusion

8. The Strategy presented here will ensure our IT systems remain fit for purpose for the next five years. Much of the cost of delivery will be covered by an existing ear-marked reserve, thereby minimising the impact on the Authority's annual revenue budget.

Phil West
IT Manager
18 November 2022

Annex

The Information Technology (IT) Strategy

Aim: *To manage and maintain the Authority's IT-based systems to the optimum standard for supporting the effective and efficient delivery of services, and to continue to develop these systems to take advantage of new opportunities and new ways of working.*

Introduction

The Authority aims to provide high quality, efficient and effective services and communications to its internal and external customers. Essential to achieving this is ready access to the information that the Authority produces or requires.

The Authority will maintain and develop a flexible, responsive and reliable IT environment to ensure convenient access to information, improve communication and collaboration. This should enable established systems to function effectively, and new initiatives to be undertaken efficiently and to the highest quality. Although new initiatives will, from time to time, emerge as requirements from the Authority's individual work programmes, this Strategy explains how the Authority's core systems will be developed over the next 5 years.

1. Principles

IT plays a fundamental role in the operations of the Authority, with the network infrastructure underpinning all services (email, access to the web, communications, administrative applications and data security). Although there will always be some restrictions on what the IT service can provide, because of financial and practical constraints, the over-arching principle is that IT should deliver what the Authority needs, rather than prescribing how the Authority should operate. This approach is underpinned by a series of more specific principles (**Appendix 1**), including those which are particularly relevant to new developments.

The following considerations have influenced the preparation of this strategy:

- The Authority's statutory purposes and objectives
- Contractual and legal considerations, including regulatory matters
- Best practice and opportunities for improvement
- Government policy
- Initiatives for developing particular services or programmes
- Leveraging maximum value from the Microsoft 365 suite of products

- Best use of resources, keeping the cost of ongoing activity as low as possible without compromising operational requirements.
- Energy efficiency and carbon footprint when purchasing new IT equipment.
- GDPR requirements

The delivery of this Strategy is supported by a series of IT policies and procedures which are kept under regular review; appropriate reference to these is made throughout the following text.

2. Current systems and future considerations

This Strategy assumes that our current IT requirements will continue to evolve due to additional operational requirements or technological advances.

The pace of change in IT since the last edition of this strategy (2016) has showed no signs of slowing; areas of particular interest include virtualised cloud environments, remote working, site working, collaboration capabilities, video conferencing, and moving to Microsoft 365 (MS365) and associated inclusive products. When a system or its contract comes up for fundamental review, we will look at the best ways of providing those services in the light of any new technologies available. Such opportunities could include joint purchasing arrangements with other National Park Authorities or Local Authorities.

The Authority has an increasing estate of mobile devices (Laptops, tablets and smartphones) which are being used outside of the corporate network to connect to our systems via a Remote Desktop System (RDS). As we move away from the aging RDS, the data on these mobile devices must be as secure as is reasonably possible. Endpoint Manager is a product within the MS365 software suite which gives remote visibility, control and security over these mobile devices. Educating staff in the risks and the best ways to mitigate them will play a significant role in this security.

Wi-Fi and mobile signals in the more remote locations continue to be unreliable, causing issues with the car park machines taking card payments. We will seek to find cost effective ways to hard wire the systems and get a more reliable payment system.

A range of mobile network providers are used through a consolidated phone contact; staff are matched with the best coverage provider in their area.

Appendix 2 identifies the major developments that will be made to the Authority's IT systems over the life of this strategy. The resources needed to deliver this activity will be included within the Authority's annual budgets.

3. Risk

Management of IT-related risk is achieved primarily through compliance with IT-related policies and procedures (**Appendix 3**), all of which are available to officers. There are also a number of generic risks that affect all of the Authority's services,

including IT (such as the availability of suitably competent staff); such risks are covered by the Authority's Risk Management process.

4. Communication of this Strategy

This Strategy will be published on the Intranet.

Document Status	
Date adopted	XX December 2022
Adopted by	F&R Committee
Lead Officer	Phil West
Date of next review	No later than December 2027 (5 years)

APPENDIX 1

The principles behind this Strategy

A. OPERATIONAL CONSIDERATIONS

(i) **Information Needs**. An understanding of the information needs of the Authority (Members, officers, volunteers and external customers) is critical to developing and maintaining successful systems, to ensure that information flows effectively through the organisation.

(ii) **Access**. All users should have access to the information they might reasonably need, via appropriate ICT systems and hardware, in order to execute their duties. Information should be accessible in an appropriate and cost-effective format and available in a timely manner. Effective management information and reporting systems are required.

Officers need to be fully aware of the legal issues surrounding information access, including the General Data Protection Regulation (GDPR), the Data Protection Act (DPA), the Freedom of Information Act, the Copyright, Designs and Patents Act and the Environmental Information Regulations.

(iii) **Information management**. Officers require access to both internally and externally generated information in order to execute their duties. We will procure such information in order to meet such needs (e.g. Geographic Information Systems (GIS) data). The general principle of information being available to all will apply, unless specifically specified otherwise (e.g. for legal, data protection or HR reasons).

(iv) **Information systems**. We will provide the systems needed to create, manage, store, access, manipulate and transmit information, at every physical location where officers are required to work. Information will be delivered to the point where it is needed, securely, accurately and on time.

(v) **Information sharing**. Information created in or imported into the Authority's systems should be capable of being accessed, shared and manipulated easily from multiple platforms and applications, or transferred easily and without loss of accuracy or quality between them. Data should be held in as few locations and systems as possible and ideally live data should originate from a single source. The increased use of MS365 will allow improved, more secure collaboration with internal and partner organisations. Officers will be trained on the data sharing capabilities and risks of MS365. All systems and data should have adequate security and back-up measures applied which are proportional to the assessed risk.

Web browser-based interfaces will be maintained to provide access to applications wherever appropriate, including Corporate Information Systems. Where web-based delivery systems are not available, consideration should be given to how users of all platforms will access information. In all cases, the risk to the security of data and applications will be a major consideration in the provision of such access.

We will seek to ensure that all systems are available to share easily, and will, for example, avoid developing systems that are only available to one site or which are suitable only for a limited number of users; this constraint excludes those areas where a bespoke service is necessary, for example Development Management, the Historic Environment Record and Finance.

(vi) **Revision and replacement of IT resources**. Budgets will be created to deal with the lifecycle of hardware and software, as well as for one-off funding of specific developments. New systems will be assessed and analysed by the project manager and IT Team to ensure they are compatible with current and emerging platforms, that they are fit for purpose, affordable and align with the future vision of the Authority.

B. PLANNING OF WORKLOAD AND FUTURE DEVELOPMENTS

(vii) **IT planning and resourcing** will aim to provide reliable facilities appropriate to help deliver the Authority's objectives. We will maintain a stable network and develop systems which enhance the Authority's effectiveness and efficiency.

(viii) **Planning and prioritising** IT developments will be undertaken in a 'joined-up' manner. Plans will be discussed and agreed, well publicised and appropriately funded, and any compatibility and data sharing issues will be discussed with partners. This Strategy provides the basis for the annual work plan of the IT team. Operational plans for the roll-out of new services will be clearly explained in advance, so that teams and individuals can plan accordingly. Appropriate training will form part of the planning process for IT developments, to ensure their proper take-up and use.

(ix) **Capacity**. All planning of IT facilities and services will take into account the implications for, and constraints on, the IT team, including workload and skills, and any external support implications. There will be measures in place to reduce diversification of equipment including printers and software, in favour of a limited set of standards and shared network devices.

(x) **The planning of new systems** will be based on reliability, compatibility with current and future operating systems, ease of upgrade and of maintenance.

(xi) **Network infrastructure** will continue to be developed with a view to long-term benefit, prudent use of new products and careful collaboration with other services. The level of user traffic will be monitored to enable adequate capacity to be planned and provided.

APPENDIX 2

Future Developments

This Appendix lists the major changes that the IT Service plans to make to the Authority's systems over the period covered by this Strategy and explains why these changes are required. A timeline for key changes is included at **Table 1**.

1. Servers

Current server infrastructure operates in a mainly virtualised environment and runs operating systems ranging from Windows Server 2012 to Windows Server 2019. There are several physical HP and Dell servers which are used as Domain Controllers and Virtual Control servers with Windows 2019 Data Centre licenses for disaster recovery.

Future Developments. Each of the older physical and virtual servers will be upgraded to Windows Server 2019 operating system by the end of 2023/24.
A refresh of the Storage Area Network (SAN) disk array which hosts the Authority's virtual servers will be needed during the life of the strategy. Options are either an in-house like for like upgrade or a fully hosted cloud system. Resilience, disaster recovery, business continuity improvement and cost will be major considerations.

2. Authority Network

2.1 Wide Area Network (WAN).

All Authority-operated premises are connected by a WAN. Yoredale and Colvend are connected by a dedicated fibreoptic connection linking the sites for RDS access, disaster recovery and server replication. The Authority has a 100mbs internet speed limit shared amongst all our sites but geographical differences in sites can still cause network speed inequality. The Authority's main telephony system also uses this data connection.

Future Developments. We are currently in an extension period of our NYNET WAN contract. The Teckal agreement behind our contract was extended by North Yorkshire County Council to end in 2024. The Authority's connectivity needs will be reassessed before this point taking into account bandwidth changes created by more remote working and the increased use of cloud services. This will give us the opportunity to take advantage of any new network management technologies and changes in connectivity.

2.2 Local Area Network (LAN).

All our offices are running on category 5e or 6 fixed wire Ethernet network, with switches rated at 1Gbs. The phone system is supported by Power over Ethernet (PoE) switches and patch panels. Yoredale core network switches will be replaced in 2025/26. Edge switches will be replaced as they reach end of life.

2.3 Wireless Access Points.

There are public wireless access points in the Malham, Aysgarth, and Hawes (Dales and Countryside Museum) visitor centres, and in the main meeting rooms at Yoredale and Colvend. There are private Wi-Fi networks at Yoredale and Colvend

for use exclusively with Authority equipment.

Future Developments. We will establish the feasibility of extending the Colvend (Grassington) Wi-Fi to the visitor centre. We will investigate point to point Wifi and the possibility of hard-wired internet connectivity to improve the reliability of our carpark machines and any potential requirements of vehicle charging points.

3. Client Machines

3.1 Hardware. Current hardware is a combination of Personal Computers (PCs) and laptops running on Windows 10 operating system. These provide access to the Authority's systems and data via Remote Desktop Services technology. Laptops, managed as a pool, are also available for officers not issued with a laptop who need to work offsite. Tablets are issued to individuals for specific tasks and software applications within the Authority.

New mobile smart devices (tablets and phones) are enrolled and managed through MS365 Mobile Device Management software.

Future Developments. All 'like' equipment will be group-purchased where possible (laptops and desktops) to achieve economies of scale and to improve efficiency and implementation times. PC's will be replaced with laptops as they come to the end of their life unless there is a strong reason to replace them with a new PC. We will make use of MS365 Endpoint Manger (included in laptop users' licenses) to remotely manage security settings, software installs and updates, and to keep data on remote devices secure.

4. Software

The Authority moved to Microsoft 365 (MS365) for all its Microsoft Office products in 2021. This is a subscription-based model which will always provide the Authority with the latest version of Office products with the latest security features.
Currently MS365 is being used for local licensing for Office on laptops, Microsoft Teams is being used as a video conferencing system and a softphone for internal calls for many staff, Microsoft Endpoint Manager and Defender (for antivirus). Underpinning the wider use of Teams and future MS365 development is our SharePoint installation. This is currently in its most basic form and holds all the data for the Agile APAS development management planning software. Mobile Device Management is being used to secure the laptops, smartphones and tablets when working outside the Authority's premises.

Future Developments. The Authority will make wider use of Teams and soft phones, instant messaging & collaboration tools. Next steps in the future developments include implementing document management (SharePoint) in 2022/23 and assisting Directorates to migrate their data in 2023/24 to replace the Authority's X:Drive and OneDrive to replace U:Drives. This will enable more secure and auditable collaboration with both internal and external partners. Management information will be available from SharePoint providing automated Document Retention, Data Protection checking and Freedom of Information Requests. Once these first stages are complete, staff will be able to take advantage of the wide range

of MS365 software and apps which are all included in the price model which will leverage the value the Authority can gain from this model.
Currently included in E3 licenses are:
Word, Excel, PowerPoint, Outlook, OneNote, SharePoint, OneDrive, Teams, Endpoint Manager, Office for Mobile, Bookings App, PowerApps for 365, Microsoft Planner, Defender Antivirus, and Audit and retention tools.

5. GIS

The Authority is part of the Public Service Mapping Agreement (PSMA), with access to a comprehensive range of maps from Ordnance Survey. We also purchase other maps and information layers from other agencies. Recording of spatial data is currently done on a variety of software and equipment. Quantum Geographic Information System (QGIS) is an open-source GIS package which runs on the RDS, laptops and tablets. It is maintained in-house by the GIS Officer with an external company providing support where required for major upgrades and development.

Future Developments. Update the Mapin App used on smartphones. The Authority's GIS Data is held onsite which could create difficulties for some remote work once the RDS is decommissioned. We will investigate options to allow remote access to our data via virtual private network (VPN), the MS365 Direct Access connector, or cloud host the data with potential savings by sharing the hosting provided by the National Parks Portal.

6. Mobile Phones

All our mobile phones were recently consolidated into one umbrella contract with multiple networks available. All smartphone devices are being enrolled on MS365 Endpoint Manager for security and remote management.
Non-smartphones are protected from data theft by a Personal Identification Number (PIN).

Future Developments. Now that all individual mobile co-terminate it will enable us to negotiate better terms when it is time to renew in 2023. Groups of apps can be published to different groups of smart-phones users depending on what they need for their roles. This will be managed centrally by MS365 Endpoint Manager. Our current mobile phone contract includes 121 connections. If external calling from softphones installed on laptops becomes an option in the future, it will be possible to reduce the number of connections the Authority needs.

Writing bespoke mobile apps in-house using MS365 Power Apps will be available to users with appropriate training. The IT Team are currently trialling an app written in-house to assist in annual asset checking.

7. Finance / Retail System

The Finance system and Retail system run separately; both systems perform the individual tasks required of them, but they have no direct interface. Consequently, there is some duplication of work activity, with information needing to be input and monitored separately in both systems.

Future Developments. There are currently no plans to integrate these systems; no one product in our price range performs the function of Finance/Retail to the required functionality. The finance system is held on virtual servers in Yoredale and is accessed via the RDS and migrating the system to the secure cloud hosted by the software vendor is currently prohibitively expensive. To enable remote working we will investigate options to allow secure remote access to finance data via virtual private network (VPN) or the MS365 Direct Access connector. The finance system will be due a major upgrade in 2025/26, we will revisit their hosted solution then.

8. Printers.

Currently we have five main Ricoh printers (multi-functional devices (MFD's)) and twenty-nine smaller desktop printers across the Authority. The current contract with the larger MFD's ends in August 2024.

Future Developments. Print costs for the larger MFD's are significantly cheaper than the older, smaller desktop machines; on renewal of the contract we will reduce the number of the smaller devices where possible. Decommissioning and consolidating the smaller printers to use more modern desktop MFD's. This will reduce printing costs as well as reducing carbon emissions.

Table 1 – Timeline

Project	Notes	Period
SharePoint Build	Setup SharePoint in preparation for migration of X:Drive	2022/23
SharePoint Migration	Work with Directorates to help them migrate their X:Drive data into SharePoint	2023/24
Servers	Upgrade to 2019	2023/24
Carpark Machines	Work with Park Services to hardwire car park machines to network	2023/24
GIS Apps	VPN for remote access	2023/24
Phones	Re-contract	2023/24
WAN	Re-tender	2023/24
Switches Bainbridge	Replacement	2023/24
Server Estate	Replacement	2024/25
Client Machines	Replace desktop hardware	2024/25
Printers	Re-tender	2024/25
Laptops	Replacement	2024/25 & 2025/26
LAN	Upgrade core switches	2025/26
Finance System	Upgrade	2025/26
Switches Colvend	Replacement	2027/28
Domain Controller	Replacement	2027/28

APPENDIX 3

IT Policies and Risk Management

The following policies provide the framework by which the Authority manages its exposure to specific IT-related risks.

It is a requirement of our induction process for new recruits that they must confirm they have read and understood these policies, and that they agree to comply with them. New or updated policies are communicated directly to existing officers. These policies (listed below) are maintained by the IT Manager and are available on the Intranet; all IT policies will be reviewed within the first 6 months of the delivery of this strategy, to make sure they remain appropriate.

- **Software Management Policy**. Sets out the means of ensuring that software is installed and used in an appropriate manner.

- **Internet Acceptable Use Policy**. Deals with the risks of internet access and sets out what the Authority has determined is unacceptable use.

- **Email Procedures and Protocols**. Describes best practice and what is considered to be acceptable behaviour.

- **Remote Access Procedure**. Describes the process to follow to achieve access. A separate Remote Access Policy, dealing with Health & Safety considerations, and management approval for off-site working, is maintained within the ‘Personnel policies’ section of the intranet.

- **Back-up and Contingency Policy**. Covers the approach to dealing with minor and major systems failures.