Job Description

1 Job details

Job title:	IT and Cyber Security Technical Officer
Team:	IT and Cyber Security
Directorate:	Resources
Post number:	TBC
Hours per week:	Up to 22
Grade:	Band 7
Base:	Lymington Town Hall
Accountable to:	IT and Cyber Security Manager
Responsible for:	No staff
Indirectly responsible for:	None
Budget Responsible Officer (BRO):	No
Car user:	Casual
Politically restricted:	No
Does this post involve working with children and/or vulnerable people?	No
Membership of professional body required:	No
Key liaisons:	New Forest National Park Authority (NPA) staff, NPA members, partner organisations, third party contractors, neighbouring local authorities, other National Park IT contacts

2 Role summary

2.1 Delivery of the effective operation of the NPA's IT infrastructure, systems and security.

2.2 Advise and make recommendations to ensure the effective implementation and development of the NPA's IT Strategy.

2.3 Maintain the NPA's centrally based and online servers, PCs, networks and applications.

3 Main duties and responsibilities

3.1 Assist the IT & Cyber Security Manager on the implementation and development of the IT strategy.

3.2 Ensure the efficient operation of corporate systems and maintain a high level of user support.

3.3 Responsibility for ensuring that appropriate hardware, software, networks and other communications equipment is provided and maintained to meet the NPA's business needs including maintenance, deployment and support of the operating systems, the creation and installation of Microsoft Intune managed applications and the administration and upkeep of the Microsoft Azure virtual servers and infrastructure.

3.4 Support and troubleshooting of network connections of all devices and associated peripheral equipment connected to the network.

3.5 Responsible for the administration of Microsoft Exchange email server and the implementation and administration of Microsoft SharePoint Online.

3.6 Maintain up-to-date knowledge of IT developments, including national and Government standards, to ensure that systems and security remain appropriate for the NPA's needs.

3.7 Ensure that the NPA's data is stored securely and is accessible within current legislation.

3.8 Assist the IT & Cyber Security Manager to ensure that back-up and recovery procedures are documented and reviewed as appropriate to support business continuity.

3.9 Advise and assist on the maintenance, development and communication of a code of practice in the use of IT.

3.10 Manage personal development, updating skills and knowledge and identifying training opportunities.

3.11 Administrate and implement Firewall policies and rules.

3.12 Helpdesk support and advice to all PC, central computer and network users, arranging for repair and data recovery when necessary, to IT and Corporate Standards.

3.13 To comply with all decisions, policies and standing orders of the NPA and any relevant statutory requirements, for example, Health and Safety at Work Act and Data Protection Act.

4 Problem solving

4.1 Responsible for IT related problems and is expected to formulate solutions in carrying out systems maintenance and support affecting all system users. This involves using technical knowledge and a range of experience to troubleshoot and create solutions that best support the teams, whilst ensuring the IT service runs smoothly.

4.2 Adapt and improve the IT support procedures, through use of initiative and interpretive thinking, to ensure users get the best out of the systems.

4.3 Using extensive research and best practice, creative thinking is required to find technical solutions that support the effective running of the NPA in line with its vision, values and budget.

4.4 As an IT expert, advise on IT policies and projects, including cost/revenue implications. Outcomes may affect the NPA as a whole in terms of service delivery and cost.

5 Decision making

5.1 Make day-to-day decisions on all IT related matters to ensure the smooth running of IT services. Only the most complex of decisions will be referred to the line manager.

5.2 Ensure service standards are maintained while thinking creatively to formulate and recommend service delivery enhancements affecting all system users.

5.3 Undertake development of server management and backup storage arrangements.

5.4 Develop procedures and be point of contact for capacity planning and emergency situations.

6 Operational responsibility

6.1 Responsible for formulating and keeping to annual programme of work, overseen by line manager.

6.2 Responsible for complex technical decisions, systems access, the security of the IT area and adhering to work service standards.

6.3 Produce reports on IT related matters for senior managers and/or members.

6.4 A requirement to be an in-house IT expert providing advice to all officers at the NPA.

6.5 There is significant access to sensitive and confidential information.

6.6 Responsible for the virtual infrastructure, SAN, network and hardware.

7 Communication

7.1 Liaise with internal staff and managers, communicating complex technical information in a clear and precise manner enabling the recipient to understand and promoting effective use of ICT throughout the organization.

7.2 Communicate with external third-party contractors, using effective influence and negotiation to ensure correct and timely delivery of service without any security breaches.

8 Working conditions

8.1 The work is office-based with home working options, though there will be occasional travel for meetings and work outside normal office hours will be required on occasions.

9 General

9.1 The post holder must at all times carry out their responsibilities with due regard to NPA policy and procedures.

9.2 All staff have a responsibility to participate in the NPA appraisal scheme and to contribute to their own development, and the development of any staff they appraise or are responsible for.

10 Job description agreement

10.1 The above Job Description is not intended to be exhaustive, the duties and responsibilities may therefore vary over time according to the changing needs of the service.

Job holder's Signature: _____ **Date** _____

Manager's Signature: _____ **Date** _____

Person Specification

IT and Cyber Security Technical Officer

Criteria	Essential	Desirable	Assessed by
Education / qualifications			
A relevant industry recognised certification related degree or equivalent (or comparable in terms of experience)	Y		A
Experience			
Demonstrable experience of supporting Microsoft Server and Microsoft 365	Y		A / I
Experience in evaluating system documentation, identifying and implementing necessary data backup and system access control procedures and restore routines	Y		A / I
Experience in administration of at least one of Microsoft Intune, Microsoft Exchange or Microsoft Azure (or similar systems)	Y		A / I
Experience in implementation and administration of SharePoint Online		Y	A / I
Experience of virtual server administration and upkeep	Y		A / I
Knowledge			
Knowledge and understanding of Microsoft Exchange, Microsoft Intune and Microsoft Azure		Y	A / I
Knowledge and understanding of Microsoft Defender Security and Conditional Access policies		Y	A / I
Knowledge and understanding of Local Government practices and procedures		Y	A
Knowledge of Microsoft 365 / Cloud		Y	A / I
Skills			
Good interpersonal and communications skills to communicate effectively with all system users.	Y		I / T
Demonstrate previous experience of working as an effective team member.	Y		I
Good customer service skills to interact effectively and professionally with external and internal customers	Y		I / T
Impact and attributes			
Ability to maintain and understand the need for confidentiality in an IT systems environment.	Y		A / I
Proven ability to respond effectively to a disaster situation		Y	A / I / T

Evidence assessed by key:

A = Application form / CV
I = Interview
T = Testing / assessment / presentation