CYBER SECURITY

Improvement & Innovation Advisory Committee – 23 June 2022

Report of: Jim Carrington-West Chief Officer Customer & Resources

Status: For information

Key Decision: No

Portfolio Holder: Cllr. Peter Fleming

Contact Officer: Amy Wilton, Ext. 7280

Recommendation to Improvement & Innovation Advisory Committee: That the report be noted.

Reason for recommendation: the report is for information only.

Introduction and Background

1 Cyber Security is the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

2 Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it is difficult to imagine how we would function without them. From online banking and shopping, to email and social media, it is more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

3 The key thing to understand about cyber security defences is that they need to be layered and include a range of measures, from technology solutions to user education to effective policies.

Measures in place

4 The Council, through the IT Services team has membership through a number of organisations, enabling access to a wider set of resources to strengthen our defence against cyber attacks.

5 A number of cyber security services are utilised through a range of organisations and internally.

6 The Council has been successful in applying for cyber security funding from the Department for Levelling Up, Housing and Communities (DLUHC). This

funding has enabled us to identify a number of areas for investment, which will strengthen our defences and reduce our risk.

7 Training has been rolled out across the organisation, with mandatory e-learning developed by the National Cyber Security Centre (NCSC) provided for all Council staff. In addition, key personnel have undertaken more in depth training tailored to specific roles within the organisation, to enhance the management of the Council's cyber security approach.

8 Independent external audits have been completed in the last 12 months, specifically looking at the Council's cyber security planning. The outcomes of these audits have provided valuable advice to focus resources internally.

Key Implications

Financial

There are no financial implications to this report.

Legal Implications and Risk Assessment Statement.

There are no legal or risk implications related to this report.

Equality Assessment

The decisions recommended through this paper have a remote or low relevance to the substance of the Equality Act. There is no perceived impact on end users.]

Net Zero Implications

The decisions recommended through this paper have a remote or low relevance to the council's ambition to be Net Zero by 2030. There is no perceived impact regarding either an increase or decrease in carbon emissions in the district, or supporting the resilience of the natural environment

Conclusions

The report is for information only and Members are requested to note the report.

Appendices

None

Background Papers

None

Jim Carrington-West

Chief Officer Customer & Resources