Corporate Policy and Resources Committee
Monday, 9 January 2023

Subject: ICT Policy Update

COMMITTEE	DIRECTORS
Corporate Policy and Resources Committee (09.02.23)	Director of Change Management, ICT & Regulatory Services

Report by:	Director of Change Management, ICT & Regulatory Services
Contact Officer:	**Cliff Dean, ICT Manager** cliff_dean@west-lindsey.gov.uk
Purpose / Summary:	To seek approval from Corporate Policy and Resources Committee of the suite of Information Technology Policies, which have been refreshed to ensure they are compliant with the new National Cyber Strategy 2022.

1. **RECOMMENDATIONS:** That Corporate Policy and Resources Committee approve the ICT Policy report and associated updated policies:
    a. Information Security Policy (Appendix 1)
    b. ICT Disaster Recovery Policy (Appendix 2)
    c. Incident Response Action Card Phishing (Appendix 3)
    d. Incident Response Action Card Denial of Service (Appendix 4)
    e. Incident Response Action Card Malware (Appendix 5)
    f. Incident Response Action Card Ransomware (Appendix 6)
    g. Network Connection Agreement (Appendix 7)
    h. Patch Management Policy (Appendix 8)
    i. Mutual Non-Disclosure Agreement (Appendix 9)
    j. Change Management Procedure (Appendix 10)
    k. Remote Working Policy (Appendix 11)
    l. Members ICT Policy (Appendix 12)
2. That ICT will communicate key changes to staff and Member's though Minerva, the Member's Handbook and the learning management system

(Learning Pool), providing the opportunity for staff to read and understand the policies and have the process confirmed.

3. That all newly elected Member's will receive a copy of the Members ICT Policy contained within the Member's Handbook.
4. That any future minor housekeeping amendments be delegated to the Director - Change Management, ICT & Regulatory Services, in consultation with the Chairs of the Joint Staff Consultative and Corporate Policy and Resources Committees.

IMPLICATIONS

Legal:

No Legal implications from this report

Financial: Fin Ref FIN/120/23/SSc.

No financial implications arising from this report.

Staffing :

None arising from this report

Equality and Diversity including Human Rights :

None arising from this report

Data Protection Implications :
Having read through the policy the DPO found some minor discrepancies however these were raised in the comments for the report owner and have been resolved.

Notes from the DPO included:

App 1 (16)(c)(i) – How will/are the authority mandating a 12-character password and how is this enforced
App 2 states - Loss of Wi-Fi (this dependency will be removed during April 2018) – should this be included
App 8 – Limitation of Liability should be re-written to be more easily readable.

The rest of the DPO notes were regarding version history, reviews, document control and revision throughout the whole police and appendixes.

However, all notes have been confirmed as actioned by the document owner and as such the DPO is happy with the policies based on this point.

Climate Related Risks and Opportunities:

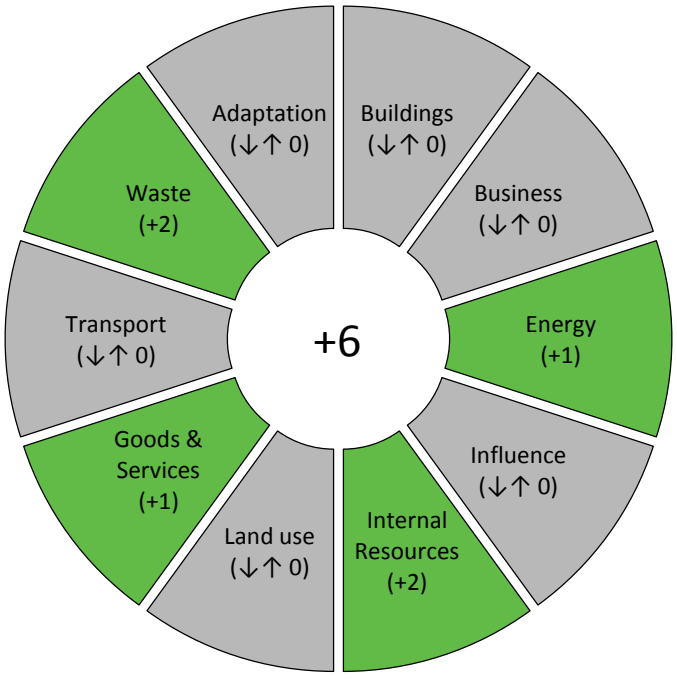
Individual climate change and environmental impact assessments will be included as part of the decision-making processes for specific spending options.

The CESIA that accompanies this report focuses on changes from the revised ICT policies rather than the overall impact of the service function. The reported impacts are considered to be substantive positive changes because they will allow us to reduce the amount of equipment we use in the future. The changes will allow us to maintain security, reduce electricity use, and promote continued support for our communities.

Should other elements of the policies come forward for delivery beyond the scope of the guiding policies these will be subject to a CESIA at that point in time, as appropriate.

There are some aspects of the project that are known at this time e.g., improvements made to the energy efficiency etc.; what is not known at this stage is the exact way that procurement elements will be designed and implemented. The Project Team will need to know this information for a full and proper assessment to be made of the impact of the project on climate change. The procurement will be discussed with the Council's Climate Change Officer and subjected to the Council's CESIA tool.

The outcomes, though provisional at this juncture, will then be considered in preparing the ground for the procurement of professional services and new equipment. A CESIA tool pie chart is shown below, which communicates pictorially the current climate change impact of the revised ICT policies based on the current status of information.



West Lindsey District Council will be net zero by 2050 (26 years and 11 months away).

Section 17 Crime and Disorder Considerations:

None arising from this report

Health Implications:

None arising from this report

Title and Location of any Background Papers used in the preparation of this report :

National Cyber Strategy 2022

https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Risk Assessment :

Risk of Cyber Attack is a strategic risk for the Council and included in the Corporate Risk Register. These policies are essential mitigating factors both in reducing the probability and impact of this risk.

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e., is the report exempt from being called in due to urgency (in consultation with C&I chairman)	**Yes**		**No**	**X**

Key Decision:

A matter which affects two or more wards, or has significant financial implications	**Yes**		**No**	**X**

1 Introduction

1.1. The Information and Communications Technology polices have been reviewed and updated to include further information around cyber security and the unique environment the Council is using including data centre, network, internet, and devices such as laptops and tablets.

1.2. The update includes details regarding not using devices for personal use, password changes for officers, multi factor authentication and risk-based logon procedures.

1.3. The updated information around business continuity and disaster recovery, sets out the approach we would use to manage a variety of possible data compromises scenarios with insider threats continuing to be biggest issue.

1.4. The Councils ICT Manager has approached Lincolnshire County Council's ICT Department and is meeting with Nicola Calver (Member Services Manager) to progress the opportunity for members that represent West Lindsey District Council and Lincolnshire County Council using one device for both authorities.

2. Technological Approach

2.1. The new policy documents are designed to bolster how we manage the Council's data. For example, where colleagues use secure technology to access work areas or conduct searches, we retain that capacity to review network traffic to ensure it is necessary in relation to the purpose for which it was originally created.

2.2. For officers, no software shall be either downloaded or installed without approval from colleagues in the Information Communications Technology Department (ICT). If there is a new software installation colleagues in ICT will review the circumstances.

3. Assurance

3.1 In order to maintain assurance, the Council is updating appropriate measures, which includes technical controls and a suite of policies, as detailed below. In addition, there will be increased employee training and monitoring.

3.2 The ICT function has had the benefit of the following audits and outcomes:

- Network Security – Substantial Assurance
- ICT Audit of Disaster Recovery – Substantial Assurance
- ICT Help Desk Audit – Substantial Assurance
- Cloud Hosted Services – Substantial Assurance

4. Changes

4.1 It is proposed that Corporate Policy and Resources Committee approve the suite of Information Communication Technology Policies, which will continue to provide assurance on our Public Services Network (PSN) connection, Payment Card Industry Data Security Standard (PCI-DSS) and our Future Networks for Government (FN4G).

4.2 The changes for each policy are as follows:

Information Security Policy (Appendix 1)
Details on how multi-factor authentication (MFA) helps the Council have been included. In relation to passwords the length of passwords has been increased, the requirement for complexity has been removed and the detail supporting three random words has been included. Details of the technical process for logging onto the network have been included that reference the conditional access, this is a risk assessment to secure colleague's user accounts. The Cloud Security Principles defined by the National Cyber Security Centre(NCSC) are included in the document and how they provide benefit. The process for starters, leavers and movers is now included as it refers to the process that is supported by the technology we manage. Employees have the right to use the equipment for work purposes only.

ICT Disaster Recovery Policy (Appendix 2)
The physical equipment used and how it works has been updated following the implementation of the new data centre. The supplier details for the new equipment and software have been updated. The ICT assets have been expanded, to now include the network and our public cloud. The technology we use (Zerto) has been included and how we use it to stop data loss for the Council.
The way the backup arrangements work has been documented to reflect we use the best practise approach (3-2-1 as recommended by the National Cyber Security Centre). The details of each monitoring tool we use has been included to evidence the value they provide to us. We have introduced Cyber Response Plans, as process documents that colleagues in ICT will use to deliver a consistent approach to dealing with cyber incidents. The invoked process has been updated to reflect the loss of our data centres, through several scenarios, which range from losing one, to losing all our data centres.

Incident Response Action Card Phishing (Appendix 3)
New procedure for ICT colleagues.

Incident Response Action Card Denial of Service (Appendix 4)
New procedure for ICT colleagues.

Incident Response Action Card Malware (Appendix 5)
New procedure for ICT colleagues.

Incident Response Action Card Ransomware (Appendix 6)
New procedure for ICT colleagues.

Network Connection Agreement (Appendix 7)
New procedure for allowing connections from third parties onto the network.

Patch Management Policy (Appendix 8)
Updated to include auditing and monitoring of patches, the updating of network infrastructure (firewalls, switches, wireless access points) and smart devices.

Mutual Non-Disclosure Agreement (Appendix 9)
New agreement that has been revised, ready for approval. The agreement is used to provide assurance from third parties when working with us on ICT.

Change Management Procedure (Appendix 10)
New procedure that the colleagues in IT will use, for managing ICT change in the ServiceDesk.

Remote Working Policy (Appendix 11)
The way users connect to the network has been updated (it's the technology we use F5). The Data Protection Act has been updated along with how colleagues in Revenues and Benefits use virtual desktops to connect to the Public Services Network (PSN).

Members ICT Policy
New Policy used in the Members Handbook, minor update on reference to device rather than tablet. Includes details on using Microsoft Office products on another device.

5. Next steps

5.1. For the development of this report and the associated updated policies they have been shared and reviewed with colleagues on the Corporate Information Governance Group (CIGG) ICT Board and JSCC ahead of this report for CP&R, dates as detailed below.

5.2. Communication and training for staff will form part of the development programme using the Councils 'Learning Pool' system. Members will be receiving full detail of the policy, it will be included in the Member Handbook and provided by the ICT team during induction in May 2023.

Management Team	09/01/23
JSCC	19/01/23
ICT Programme Board	24/01/23
ICT Partnership Board	09/02/23
CP&R	08/03/23
Staff Engagement	01/04/23