Warwickshire Fire and Rescue Service Firefighter Pension Schemes

Cyber Security Policy

1. Introduction

Warwickshire County Council holds personal information for more than 1,000 members of the Firefighter pension schemes (“the Schemes”). The Schemes hold large amounts of personal data which can expose them to significant risks if an error occurs.

A Cyber Security Policy for the Schemes is set out below and a summary of the guidance from the Pensions Regulator is included at Appendix 1.

2. Warwickshire Fire and Rescue Service Firefighter Pension Schemes Cyber Security Policy

1. The Cyber Security Policy is to be approved by the Staff and Pensions Committee.

2. The Cyber Security Policy is to be reviewed annually, or sooner if circumstances require it. Appendix 4 sets out roles and responsibilities to achieve this.

3. The Schemes adopt the Cyber Security protocols of the Administering Authority (Appendix 2 and Appendix 5) except where this policy expressly deviates from them or adds to them.

4. External agencies providing services to the Schemes are required to provide assurances that they have identified Cyber Security Risks and have in place arrangements to control and mitigate risks, and arrangements to report cyber security events to the Scheme Manager in a timely way. Appendix 3 sets out the external agencies.

5. Future contracts taken out with external agencies will consider how to have appropriate regard to cyber security risks in both the service specification and

contract terms.

6. Cyber security will be considered in the development and design of annual training plans for pensions administration officers and for Committee and Board members.

7. Data breaches will be managed using the Administering Authority procedure. All data breaches will be reported to the Assistant Director (Finance /scheme manager) and will be escalated if/as appropriate to the Monitoring Officer. The Monitoring Officer in conjunction with the Assistant Director of Finance will make a decision on referral to the Information Commissioner's Office and / or The Pensions Regulator as required by each entity.

8. Communications to members will from time to time include references to maintaining awareness of cyber/online fraud to assist members in protecting themselves.

9. The Schemes' risk register will have regard to Cyber Security Risk.

10. The Schemes will commission an independent audit of its exposure to and management of Cyber risks to begin within one year of the initial commencement of this policy.

Appendix 1

The Role of The Pensions Regulator

For local authority pension funds, including Firefighter Pension Schemes, the Pensions Regulator (TPR) requires pension administrators, pension committees and the local pension board to ensure that they have the appropriate system in place to ensure safe management of the schemes and custody of assets.

The Pensions Regulator summarises its expectation of pension schemes as follows:

1. Trustees and scheme managers are accountable for the security of scheme information and assets
2. Roles and responsibilities should be clearly defined, assigned, and understood
3. You should have access to the required skills and expertise to understand and manage the cyber risk in your scheme
4. You should ensure sufficient understanding of the cyber risk: your scheme's key functions, systems, and assets, its "cyber footprint", vulnerabilities and impact
5. The cyber risk should be on your risk register and regularly reviewed
6. You should ensure sufficient controls are in place to minimise the risk of cyber incident around systems, processes, and people
7. You should assure yourselves that all third-party suppliers have put sufficient controls in place. Certain standards and accreditations can help you and your suppliers demonstrate cyber resilience
8. There should be an incident response plan in place to deal with incidents and enable the scheme to swiftly and safely resume operations. You should ensure you understand your third-party suppliers' incident response processes
9. You should be clear on how and when incidents would be reported to you and others including the regulators
10. The cyber risk is complex and evolving and requires a dynamic response. Your controls, processes and response plan should be regularly tested and reviewed. You should be regularly updated on cyber risks, incidents, and controls, and seek appropriate information and guidance on threats

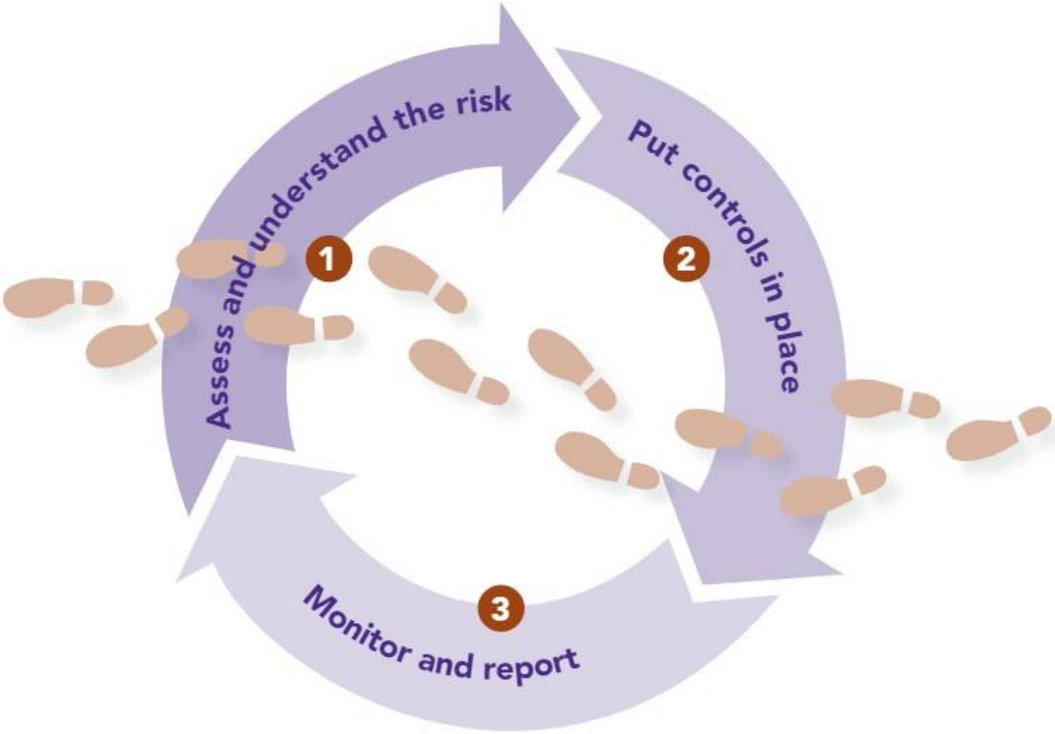
The guidance can be found in full in the link below:

https://www.thepensionsregulator.gov.uk/en/document-library/regulatory-guidance/cyber-security-principles-the-pensions-regulator

The Pension Regulator's 'Cyber risk assessment cycle has been reproduced below:

Cyber risk assessment cycle

Are roles and responsibilities clearly defined, assigned and understood?



1

Assess and understand the risk

- Do you understand the cyber risk facing your scheme:
  - your key functions, systems and assets
  - your cyber footprint, vulnerabilities and impacts?
- Is the cyber risk on your risk register and is it regularly reviewed?
- Do you have access to the right skills and expertise to understand and manage the risk?

2

Put controls in place

- Are sufficient controls in place to minimise the risk of a cyber incident occurring:
  - IT security controls
  - processes
  - people?
- Have you assured yourselves of your third party providers' controls?
- What standards or accreditations help you or your suppliers demonstrate cyber readiness?
- Do you have an response plan in place to deal with any incidents which occur and help you swiftly and safely resume operations? Do your suppliers?
- Are you compliant with data protection legislation (including readiness for the General Data Protection Regulation)?

3

Monitor and report

- Are your controls, processes and response plans regularly tested and reviewed?
- Are you clear on how and when incidents would be reported to you and others including regulators?
- Are you kept regularly updated on cyber risks, incidents and controls?
- Are you keeping up to date with information and guidance on threats?

Appendix 2

Cyber Policies of the Administering Authority

As the Administering Authority, Warwickshire County Council already has in place Information Security Policies (Cyber Security Policies) which apply to the Schemes and provide the backbone of the Cyber Security infrastructure required by the them.

https://apps.warwickshire.gov.uk/api/documents/WCCC-1162-15

Appendix 3

External Service Providers

External service providers will be required to provide assurances as to the cyber risks and arrangements to mitigate, manage, and report them. External providers include but are not limited to:

- Pensions Administration Provider
- Pension Administration System Provider
- Firefighter Pensions Payroll Provider

Appendix 4

Roles and Responsibilities

Activity	Responsible Person / Forum
Reporting cyber security failures	All
Following IT security protocols and the pension fund Cyber Security Policy	All
Maintaining a Cyber Security Policy	Pensions Policy and Governance Officer
Approving a Cyber Security Policy	Staff and Pensions Committee
Reviewing specific cyber risks – detailed risk reviews	Managed at team or contractor level, for example the pensions administration provider, the the pensions administration system provider, the firefighter pensions payroll provider,etc.
Maintaining an appropriate cyber security profile on the pension fund risk register	Pensions Policy and Governance Officer
Maintaining an up to date IT Security Policy for the Administrating Authority Generally	Warwickshire County Council Information Security Officer
Reporting data breaches and incidents	Pensions Administration Delivery Lead or the Pensions and Investment Manager

Appendix 5

Incident Reporting Process / WCC Incident Process

Below is an extract from WCC’s Information Security Policy

13. Security Incident Management

WCC recognises that from time to time ‘things go wrong’ and there may be a breach of security involving information or equipment holding information. The purpose of the “Data Breach and Information Security Incident Procedure” is to ensure that all actual or potential information security incidents are reported centrally to enable WCC to react quickly and effectively to minimise the impact.

These procedures are mandatory and must be followed by all staff as part of the council’s Information Governance Framework which is the standard for managing information in the council and is one of the linked procedures in the Information Compliance Policy aimed at all staff.

Please consult WCC’s Data Breach and Information Security Incident Procedure for more detail

https://apps.warwickshire.gov.uk/api/documents/WCCC-1073-648