THE ROYAL COUNTY OF BERKSHIRE PENSION FUND

lgps | Local Government Pension Scheme

Cyber Security Policy

Royal County of Berkshire Pension Fund

September 2026

Version History

Version Number	Revision Date	Author(s)	Change
V1.0	09/2026	Philip Boyton, Deputy Head of Pension Fund	Document creation Approved by Pension Fund Committee – 21 September 2026 Next review date – August 2027

Contents

Version History 2
Introduction 4
- **Regulatory Framework** 5
- **Scope** 5
- **Responsibilities** 5

Core Principles 6
Individual actions 6
- **Principle of personal responsibility** 6
- **Policies** 7
- **Physical security** 8
- **Circulation of Fund data** 8
- **Mobile working and removable media** 8
- **Incident Response Plan** 10
- **Information disposal** 10
- **Training** 10

Working with administering authority 10
- **Other third parties and employers** 11

Identifying a security incident 12
- **Impact** 13

Incident response plan (overview) 13
- **UK GDPR and Data Protection Act 2018** **14**
- **ICO Notification Requirements** **14**
- **National Cyber Security Centre (NCSC) Engagement** **15**
- **Law Enforcement Reporting** **15**
- **Regulatory Communications and Record Keeping** **15**

Assess and Solve, Monitor and Review 16
- **Monitor** 17
- **Review** 17

Contact details 18

Introduction

The Royal Borough of Windsor & Maidenhead (“RBWM”), as administering authority of The Royal County of Berkshire Pension Fund (“the Fund”) recognise that:

- Pension schemes are an attractive target for cyber criminals because the administering authority (and other third parties) hold valuable personal data including employment and financial data.
- Security breaches or cyber-attacks can have serious consequences for scheme members, including identity theft, loss of data and loss of assets.
- As data controller under the data protection laws, administering authorities must make sure that they have proper systems and policies in place and that any third-party suppliers (such as administration software providers, investment fund managers) also have adequate policies and procedures in place.

The potential implications of a cyber-attack on the Fund and its stakeholders can be significant and wide-ranging e.g., financial, operational and reputational. The purpose of this policy is to support the protection of the integrity and confidentiality of information held by RBWM (“the administering authority”) in relation to the Fund, in particular, the personal data of the Fund’s scheme members ("Fund data") from potential threats, whether internal or external, deliberate or accidental. Financial losses incurred because of a cyber-attack can also be significant.

This policy will help to minimise the risk of disruption to the operation of the Fund due to the loss or corruption of Fund data, and to minimise the risk of scheme members' personal data being unlawfully obtained or processed. This policy is also designed to help the administering authority meet the internal controls requirements in relation to cyber security.

The administering authority recognises its legal obligations under data protection legislation, which requires them to take steps to protect Fund data, and this policy is intended to contribute to compliance with such legal obligations.

Whilst several of the Fund’s operations fall under the policies and processes of RBWM itself in its capacity as the administering authority, the Fund is ultimately accountable for ensuring the internal/external cyber security arrangements are assessed, managed and mitigated.

Further comments on the alignment between the Fund and RBWM is set out in this policy document.

Regulatory Framework

The Pensions Regulator (tPR) issued updated guidance in 2023 on cyber security including a stronger emphasis and high-level process that pension schemes should continually follow and the principles they should adhere to. The principles set out in the guidance can be split into three main areas of focus, as shown below. The guidance can be found here.



TPR's General Code of Practice includes a Cyber Controls Module, which confirms the requirement for public service pension schemes such as the Local Government Pension Scheme ("LGPS") to establish and operate adequate internal controls that manage cyber risk. The expectations set out in the code cover two key themes - **"Assessing Cyber Risk"** and **"Managing Cyber Risk".** In setting this policy, the Fund seeks to address the issues set out in the principles and themes referred to above.

Scope

This policy applies to all Fund Officers and to Members of the Local Pension Board and Pension Fund Committee and Pension Advisory Panel. Other third parties will be made aware of this policy (including the administering authority) to ensure that the requirements set out in the policy are met.

Responsibilities

Within the Fund, the Deputy Head of Pension Fund has overall responsibility for ensuring this policy is adhered to. They are also designated as one of the Fund's Incident Response Co-Ordinators in the Fund's separate Business Continuity and Service Recovery Plan.

Given they have been delegated overall responsibility for managing the Fund, the Pension Fund Committee and Pension Advisory Panel will need to be satisfied that the Fund is meeting its cyber-security requirements and managing this risk. The Local Pension Board will have oversight of this policy and can assist the Fund and the Pension Fund Committee and Pension Advisory Panel in ensuring cyber security requirements are met.

Given the close links between the Fund and the administering authority, the responsible Officer for the administering authority policies is the Information Governance Manager and Data Protection Officer (DPO).

All persons under the scope of this policy are responsible for reporting any apparent shortcomings of security measures in relation to Fund data currently in force. Reports should be made to the Deputy Head of Pension Fund.

Core Principles

The persons set out above will use all reasonable endeavours to:

- Follow the principles set out in this policy to ensure their own actions do not cause or facilitate a security breach.
- Address cyber security risks with relevant third parties.
- Ensure that contracts with third parties contain suitable provisions covering cyber security.
- Ensure that they can identify when a security breach has occurred; and
- Follow the incident response protocol summarised in this document when a breach has occurred in line with the Fund's incident response plan.
- Ensure cyber risk forms part of the Fund's overall approach to risk management through regular consideration of the risk register and periodical review of this policy.

Individual actions

Principle of personal responsibility

Every person has a personal responsibility to take all reasonable steps to avoid information security breaches.

Policies

The Fund Officers and Councillors of the administering authority should follow the administering authority's own policies in relation to data security. The administering authority's Information Security policies should be adhered to and for those stakeholders with access to the administering authority's intranet.

In summary, the administering authority's policies cover the following:

- Clear desk policy
- Use of email policy
- Information handling policy
- Information technology access security policy
- Remote working security policy
- Care of council owned equipment policy
- Issuing of Council portable IT devices
- Accessing the FortiClient VPN from home
- Security code of conduct template
- Reporting security incidents policy
- Data transfer agreement
- The receipt of external data on portable computer media
- Secure data transfer to other organisation policy
- Storage of information
- Record retention destruction policy
- Secure storage handling, use retention disposal of disclosure information policy
- Data protection policy 2021
- Social media policy
- Use of Microsoft Teams policy
- Artificial Intelligence (AI) policy

For those Local Pension Board (including retired scheme member representatives) and Pension Fund Committee and Pension Advisory Panel Members who aren't employed by the administering authority, for consistency, they are encouraged to follow the administering authority's policies where possible (or at least policies of their own employer, where available to them) to manage their own cyber risk. As a general guide, the Fund expects the following to apply:

Physical security

- Every person has a personal responsibility to take all reasonable steps to protect the physical security of Fund data.
- All persons subject to this policy shall ensure that:

    - hard copies of Fund data are only taken out of a person's workplace where this is essential to the performance of their role. This also applies where the person works remotely for some or all the time, the person's home or personal office.
    - copies of Fund data are not to be left unattended in a place where they could be accessed by individuals not authorised to access the data.
    - Fund data is not viewed in a place where it could be seen by persons not authorised to access it, or discussed in a location where the information could be overheard by persons not authorised to access it.
    - where a person stores hard copies of Fund data remotely at home or in a personal office, the person shall take all reasonable security measures to protect such hard copies of Fund data.

Circulation of Fund data

When a person supplies Fund data to another person or a third party (whether in hard copy or electronic form), each person shall apply the following principles:

- data provided should be limited to that which is needed to perform the service or undertake the required action.
- data should be provided on an anonymised basis where this is sufficient to enable the service to be provided or the action to be completed; and
- electronic documents containing membership data should be shared securely, for example, by password protected communication with password details notified in a separate communication (and, where practicable, via a different means of communication).
- where a third party makes a secure portal available for the purposes of messaging or uploading of data, the third party process will be followed.

Mobile working and removable media

- Fund Officers and Councillors of the administering authority must only use their administering authority email account to send and receive emails relating to the Fund

and must not forward any e-mails regarding Fund business to any other email accounts they hold.

- where Local Pension Board and Pension Fund Committee and Pension Advisory Panel Members (who aren't from the administering authority) do not use a separate recognised email account that is used solely for Fund business and for no other purpose, they should use only a recognised e-mail account and notify the Deputy Head of Pension Fund if this address changes or if this e-mail account has been compromised in any way. They shall ensure that such email account is password protected and that the device/devices commonly used to access such email account are protected with a password or a fingerprint or facial recognition feature.
- mobile telephones which are used to access email accounts to which Fund data may be sent must be protected with a password or a fingerprint or facial recognition feature. Any administering authority devices must be used in accordance with the administering authority's policies.
- portable devices such as laptops and tablets that are used to access Fund data must be protected with a password or a fingerprint or facial recognition feature and must be kept in locked storage when not in use. Locked storage for these purposes includes:
    - an office to which access is physically restricted.
    - the individual's home; or
    - if necessary to leave a portable device temporarily unattended in a vehicle, out of sight in a locked boot.
- Fund Officers and Councillors shall only use electronic devices provided by the administering authority for Fund business unless use of a personal device has been approved by the administering authority and its use is in accordance with the administering authority's policies.
- Fund Officers and Councillors who access the administering authority IT network from outside the administering authority's premises shall ensure that they comply with the administering authority's policies.
- a dedicated website exists where Local Pension Board and Pension Fund Committee and Pension Advisory Panel papers are held, including exempt papers.
- Fund data may only be loaded on to a USB stick or other removable media where this is absolutely essential, and where this is compliant with the administering authority's policies.
- theft or loss of any device or media (including hard copy documents) on which Fund data is held should be reported immediately to the Deputy Head of Pension Fund in accordance with the separate Business Continuity Plan and Service Recovery Plan.

Incident Response Plan

The Fund has separately prepared a Business Continuity and Service Recovery Plan, which must be followed in the event of a breach of this policy, cyber-attack or other data breach. This plan considers the processes adopted by the administering authority.

Information disposal

- any persons disposing of computers, removable media or devices used for storage of Fund data is responsible for ensuring that such disposal does not compromise the security of the Fund data and comply with cyber/information security policies where appropriate.
- any confidential paper waste should be destroyed in a manner that will not compromise confidentiality, e.g., shredding.

Training

To ensure Members of the Local Pension Board (including retired scheme member representatives) and Pension Fund Committee and Pension Advisory Panel have knowledge and understanding of cyber security risks:

- the Fund requires them, together with Officers, to undertake cyber security training provided by the administering authority at least annually.
- this takes the form of general training on cyber security and specific training on data protection or cyber security risks. For those who aren't employed by the administering authority, for consistency, they are encouraged to follow the administering authority's policies where possible (or at least policies of their own employer, where available to them) to manage their own cyber risk.
- this document will inform part of the Training Strategy and help maintain good governance.
- The Fund may also consider whether any training/guidance is required for other third parties to ensure they are able to comply with the Fund's policies e.g., support for employers etc.

Working with administering authority

As referred to above, whilst several of the Fund's operations fall under the policies and processes of RBWM itself in its capacity as the administering authority, the Fund is ultimately

accountable for ensuring the internal/external cyber security arrangements are assessed, managed and mitigated.

The Fund therefore will take the following steps as part of working closely with the administering authority:

- establish a Service Level Agreement between the Fund and the administering authority documenting all external requirements placed on the Fund and the requirements for regular submission of supporting evidence.
- request regular (i.e., quarterly) reporting from the administering authority on compliance requirements to demonstrate that cyber controls are working effectively in practice. This could include reporting of any testing / back-up processes that take place.
- meetings between the Fund and the administering authority to discuss any outstanding actions / mitigations.

Other third parties and employers

The Fund requires all third-party service providers who are appointed to provide services to the Fund and who, as part of the provision of such services, will have access to Fund data, to implement and abide by appropriate and stringent processes and procedures to ensure the security of the Fund data whilst it is in their possession.

The Fund therefore endeavours to:

- consider the third party's data protection and security systems and policies when selecting the supplier or reviewing or negotiating a contract.
- consider exposure to third parties to understand the maturity of third-party security controls and check the extent to which the Fund has adequate provisions included in contracts with third parties for these controls.
- ensure that risks to scheme members data are mitigated in accordance with best practice, and that plans are in place to cover the discontinuance of the third party's business.;
- where appropriate, work with the third party to ensure that the right controls are in place (such as training and reporting).

Controls with third party suppliers should usually include:

- asking the supplier to provide a copy of its cyber security policy.
- undertaking an appropriate level of due diligence on the supplier, including the supplier's business continuity arrangements.
- ensuring the supplier is compliant with appropriate cyber security standards (such as ISO 27001) and the data protection principles.
- ensuring the contract contains suitable cyber and data protection provisions to ensure it complies with data protection legislation.
- requiring the supplier to notify the administering authority immediately on becoming aware of a security incident.

The Fund should, to the extent relevant, implement similar steps to those set out above in relation to scheme employers who transfer data to, or receive data from, the Fund.

To aid with managing and monitoring third parties, the Fund will establish a framework to record the information provided by third parties in relation to the above and to summarise the different systems/data flows in force between organisations and the frequency of data movements. This will include how data flows through the administration system software systems.

This will help the Fund establish a proportionate approach to reviewing/monitoring third party arrangements. As a minimum, the arrangements with all third parties shall be reviewed every three years. Depending on the volume of data held / processed, the Fund may also review some arrangements more frequently i.e., annually. These details will be set out in the framework.

Identifying a security incident

A security incident could include any of the following:

- loss or theft of paper files.
- loss or theft of phones, laptops, USB sticks.
- unauthorised access to computer systems or premises.
- disclosure of information to unauthorised persons.
- any sign of a computer virus or malicious software.
- security threats such as computer system failure, denial of service, or scams to gather scheme information or personal data online or over the phone.
- ransomware demands made by a third party or cyber extortion threats.

Impact

The Fund acknowledges that in addition to the direct implications of a cyber incident there will be consequential impacts relating to the rectification of the incident which can include:

- increased administrative burden e.g., communicating to members / responding to queries.
- replacement assets / system upgrades.
- regulatory exposure / potential for financial settlements.
- reputational damage.

On occasions, the Fund, alongside the administering authority, may seek to quantify the financial impact of potential cyber incidents to help inform future policy reviews (and potential cyber insurance should this be warranted).

Incident response plan (overview)

If a person becomes aware of a security breach, they must report it to the Deputy Head of Pension Fund as soon as possible who will stand up the Service Incident Response Team (SIRT) where appropriate.

The SIRT is made up of senior Pension Fund Officer and will work closely with the administering authority / third party provider(s) as appropriate and be part of any decision-making process to agree remedial actions as necessary. This will include considering what information needs to be disseminated about the incident and deciding what updates (and when) are provided to certain stakeholders.

The Deputy Head of Pension Fund should then take the following steps:

- inform the Chairs of the Local Pension Board and Pension Fund Committee and Pension Advisory Panel.
- where necessary notify breaches to the administering authority's DPO who will determine whether a report needs to be made to the Information Commissioners Office (ICO). The Administering Authority's Executive Director of Resources and Section 151 Officer will determine whether a report needs to be made to The Pensions Regulator (tPR)

- working closely with the administering authority and/or third party stakeholders, assess the immediate risks and priorities, taking specialist advice where appropriate (e.g., from specialist IT advisers).
- investigate and, in accordance with legal advice, document the extent of the breach.
- if applicable, notify and co-operate with law enforcement authorities.
- document, where appropriate, all internal/external communications relating to the incident.
- Communicate appropriately, following legal advice, with relevant parties (including employers, members and other stakeholders).

UK GDPR and Data Protection Act 2018

Where a cyber security incident results in a personal data breach, the administering authority's DPO shall be notified immediately to undertake an assessment of the breach in accordance with UK GDPR and the Data Protection Act 2018.

The assessment shall consider:

- The nature of the personal data involved.
- The volume of data affected.
- The number of individuals impacted.
- The likelihood and severity of harm to data subjects.
- Whether confidentiality, integrity or availability of Fund data has been compromised.
- Any requirements to notify affected individuals.

An initial assessment shall be completed as soon as practicable and, where possible, **within 24 hours** of the incident being identified.

ICO Notification Requirements

Where the breach is likely to result in a risk to the rights and freedoms of individuals, the administering authority shall notify the Information Commissioner's Office (ICO) without undue delay and, where required, **within 72 hours** of becoming aware of the breach.

All decisions relating to notification or non-notification shall be documented and retained as part of the incident record.

National Cyber Security Centre (NCSC) Engagement

The Fund and administering authority shall consider engagement with the National Cyber Security Centre (NCSC) where a cyber security incident:

- Results in significant disruption to pension administration services.
- Involves ransomware or cyber extortion.
- Represents a suspected or confirmed compromise of critical systems.
- Involves a significant data breach affecting scheme members.
- Indicates malicious activity by organised cyber criminals or state-aligned threat actors.
- Has the potential to impact other LGPS organisations or public sector bodies.

Where appropriate, specialist advice and support shall be requested through established NCSC reporting channels and public sector cyber resilience arrangements.

Law Enforcement Reporting

The Fund shall, through the administering authority and relevant third-party providers where appropriate, consider reporting incidents to law enforcement where criminal activity is suspected.

Incidents that may warrant reporting include:

- Ransomware attacks.
- Business email compromise.
- Fraud or attempted fraud.
- Unauthorised access to systems or accounts.
- Theft of devices containing Fund information.
- Cyber extortion demands.
- Significant malicious cyber activity targeting Fund systems, suppliers or members.

Regulatory Communications and Record Keeping

All cyber security incidents shall be documented and retained in accordance with the Fund's records management and information governance requirements.

Incident records shall include:

- Date and time of detection.
- Description of the incident.
- Systems, services and information affected.
- Actions taken to contain and remediate the incident.
- Regulatory assessments undertaken.
- Notifications made to regulators, law enforcement agencies, third parties and affected individuals.
- Lessons learned and improvement actions identified.

Reports may be made through Action Fraud, local police services, the National Crime Agency (NCA), the National Cyber Security Centre (NCSC), or other appropriate law enforcement organisations depending on the nature and severity of the incident.

The decision to engage law enforcement shall be made in consultation with senior management, information governance specialists, legal advisers and relevant technical specialists.

Following resolution of the breach, the Fund will undertake a detailed debrief to determine whether any processes and policies, and any relationships with third party stakeholders, should be reviewed.

Assess and Solve, Monitor and Review

As is the case with any risk, cyber risk demands evolving internal controls and ongoing monitoring given the pace at which cyber threats change.

Assess and Solve

Whilst putting this policy together Officers completed Aon's free Cyber Scorecard to help identify how the Fund compares with best practice, other LGPS Pension Funds, who have already completed the Cyber Scorecard, and tPR's expectations.

The assessment, designed for public sector pension schemes, consisted of around 60 questions and took around 30 minutes to complete with questions designed so that they can be completed by a typical LGPS Officer and did not require detailed technical and cyber knowledge.

The results of the Cyber Scorecard remained outstanding at the time this policy was made, the outcome will be used by Officers to develop further plans to mitigate against future cyber incidents occurring internally but also to work more closely with the Fund's providers to gain assurance about their measures in place to mitigate against future cyber incidents.

Monitor

As set out in this policy, the Fund's approach to managing cyber risk will require certain elements of the policy to be monitored on a regular basis e.g., assessment of third-party stakeholders, training requirements and individual stakeholder cyber hygiene.

Cyber security is included on the Fund's risk register. Using the action plan referred to above, the register will be updated and maintained by Fund Officers on a regular (e.g., quarterly) basis. Along with other items on the register, cyber security will be considered on a regular basis at Local Pension Board and Pension Fund Committee and Pension Advisory Panel meetings.

Review

As a minimum, the terms of this policy must be reviewed and revised, as necessary, annually, unless circumstances give rise to an earlier review of the Fund's approach to assessing and managing cyber risk e.g., legislative/regulatory change.

Contact details

The Royal County of Berkshire Pension Fund is a data controller under data-protection law. This means we store, hold and manage your personal information in line with statutory requirements to enable us to provide you with pension administration services. To enable us to carry out our statutory duty, we must share your information with certain bodies but will only do so in limited circumstances. For more information about how we hold your information, who we share it with and what rights you have, you can ask for this information from the Fund, please visit www.berkshirepensions.org.uk

If you can read this but know someone who cannot, please contact the Deputy Head of Pension Fund by e-mail – philip.boyton@rbwm.gov.uk – so we can provide this information in a more suitable format.

Office hours	
Monday to Thursday	9am to 5.00pm
Friday	9am to 4.30pm

Contact details	
Email:	info@berkshirepensions.org.uk
Website:	www.berkshirepensions.org.uk
Telephone:	01628 796668
Address:	The Royal County of Berkshire Pension Fund, Zone C Town Hall, St Ives Road, Maidenhead, Berkshire, SL6 1RF.