CYNGOR BWRDEISTREF SIROL
RHONDDA CYNON TAF
COUNTY BOROUGH COUNCIL

COMMITTEE SUMMONS

C Hanagan
Service Director of Democratic Services & Communication
Rhondda Cynon Taf County Borough Council
The Pavilions
Cambrian Park
Clydach Vale, CF40 2XX

Meeting Contact: Yula Kampouropoulou- Democratic Services (07747485569)

YOU ARE SUMMONED to a meeting of **GOVERNANCE AND AUDIT COMMITTEE** to be held at the on **MONDAY, 7TH FEBRUARY, 2022** at **5.00 PM.**

Non Committee Members and Members of the public may request the facility to address the Committee at their meetings on the business listed although facilitation of this request is at the discretion of the Chair. It is kindly asked that such notification is made to Democratic Services by Thursday, 3 February 2022 on the contact details listed above, including stipulating whether the address will be in Welsh or English.

<div align="center">AGENDA</div>   **Page No's**

4.   **STRATEGIC RISK REGISTER UPDATE: INFORMATION MANAGEMENT**

3 - 22

<u>**Service Director of Democratic Services & Communication**</u>

<u>**Circulation:-**</u>

County Borough Councillors:
Councillor M Adams, Councillor J Barton, Councillor J Cullwick, Councillor G Davies, Councillor J Edwards, Councillor M Griffiths, Councillor M Norris, Councillor D Owen-Jones, Councillor S Powell, Councillor S Rees, Councillor S Trask, Councillor E Webster and Councillor R Williams

Lay Member: Mr C Jones

This page is intentionally left blank

Information Management

A presentation:

- On the responsibilities of the Council for compliance with data protection legislation and the management of existing information management arrangements across Rhondda Cynon Taf.

- Support the Governance and Audit Committee's role in overseeing the Council's Risk Management arrangements and strategic risks as included within the Strategic Risk Register

Louise Evans,
Swyddog Diogelu a Gwella Data/Data Protection & Improvement Officer
07 Chwefror/February 2022

RHONDDA CYNON TAF

Information Management Arrangements

- Strategic Risk Register – Information Management

- Role of the Information Management Team

- Who we support

- Who we are

- Legal drivers

- ICO 'GDPR Accountability Framework'

- How we comply

- Key priorities for 2022-23

- Questions

RHONDDA CYNON TAF

Strategic Risk Register – Information Management

RISK DESCRIPTION	CONTROLS & ACTIONS	Risk Rating 2021/22			QTR 2 UPDATE 2021/22
		I	L	RATING	
If the Council does not manage its information assets in accordance with requirements set down within legislation then it may be faced with financial penalties and possible sanctions that hinder service delivery.	**CONTROLS** • Governance Structures are in place and the Council has a designated SIRO. • Policies and Procedures are in place. • Designated team in place that provides on-going training and also undertake investigations that involve potential breaches. • External Reviews & Accreditation e.g. PSN, PCI, AUDIT WALES. **ACTIONS** • Continue to review technology measures and update as necessary. • Continue to investigate and report potential events/incidents. • Continue with external reviews and maintain accreditations for PSN/PCI. • Deliver risk-based training / regular communication, face to face and via e-learning, staffing bulletins, global emails.	5	2	10	ORIGINAL RISK RATING: 4x3=12 The Information Management Team continues to provide specialist advice, information and support to Services during the quarter, ensuring that business processes are GDPR compliant - thus minimising the risk of a personal data breach and enforcement action by the Information Commissioner. Cyber Security remains a priority for the Service following increased reports of external attacks to government, local authorities and Schools. The Council is continuing with its proactive approach to mitigate risk around cyber security. Key deliverables during the quarter include: • Password Management standard strengthened in line with industry standards and technical deployment to Users commenced. • Deployment of Conditional Access policy for Microsoft Office365 commenced. • Work in progress to enhance Staff & Member Cyber Training. • Draft Cyber Incident Response Plan developed. No change to the risk ratings at this stage.

RHONDDA CYNON TAF

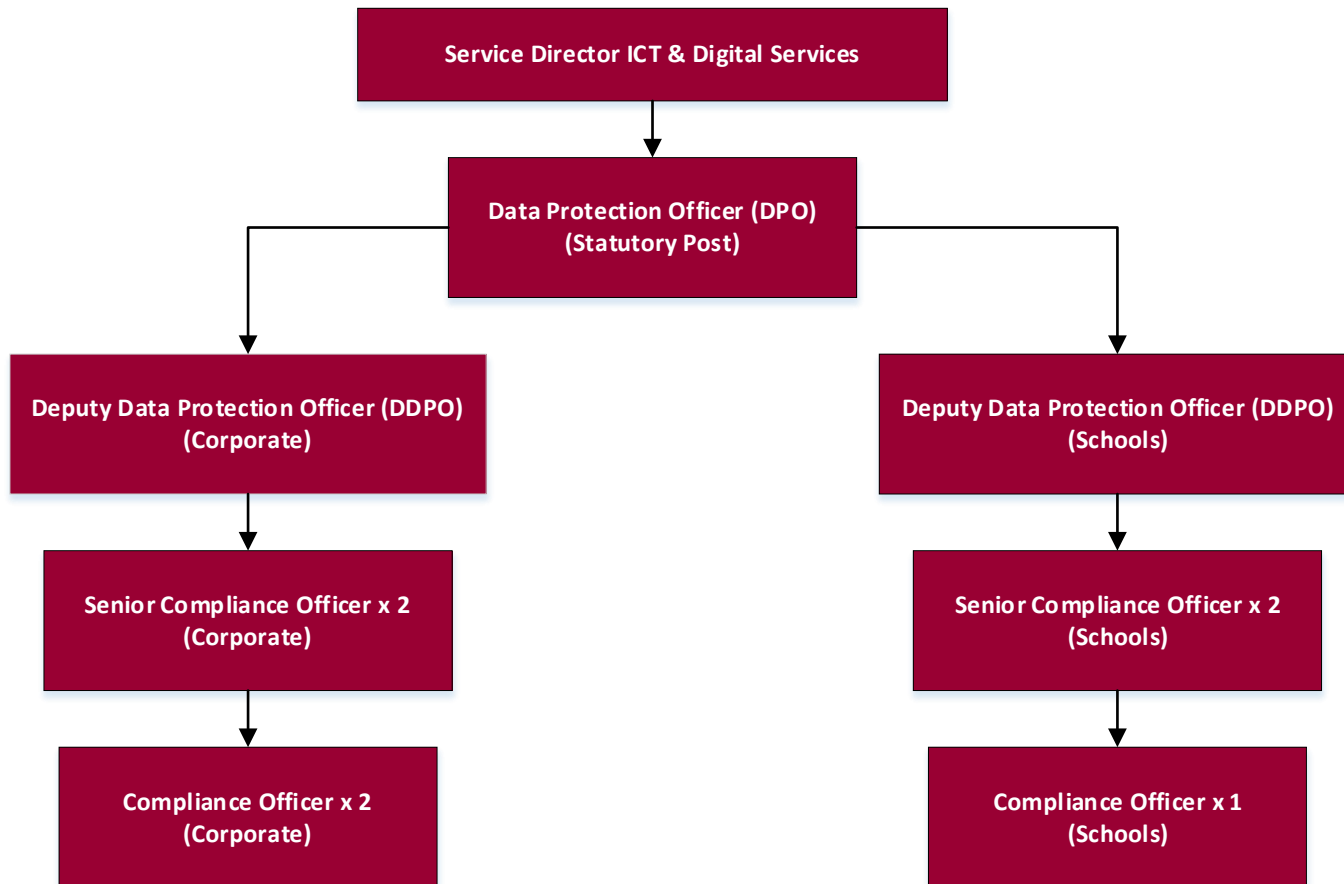# Role of the Information Management Team

Support the Council and SLA Services in achieving compliance with data protection legislation;

- Provide specialist data protection advice, support and guidance
- Manage information security incidents/events – personal data breaches
- Manage information rights requests e.g. subject access requests
- Maintain the Data Protection Register
- Conduct Data Protection Impact Assessments (risk assessments)
- Support collaborative working – advise on data protection governance arrangements, develop information sharing protocols etc.
- Develop policies, procedures and guidance
- Develop privacy notices
- Develop and deliver data protection training and awareness

RHONDDA CYNON TAF

Information Management Team - Who we support

- All Council Services

- 113 Schools

- Elected Members – Ward Cllr & Representative of the Council

- Central South Consortium

- South Wales Central Area Coroner's Services

- South East Wales Corporate Joint Committee

- The public – citizens, service users, visitors etc.

RHONDDA CYNON TAF

Information Management Team - Who we are

```
┌─────────────────────────────────────┐
│  Service Director ICT & Digital Services │
└─────────────────────────────────────┘
                    │
                    ▼
        ┌───────────────────────────┐
        │  Data Protection Officer (DPO) │
        │       (Statutory Post)        │
        └───────────────────────────┘
          │                       │
          ▼                       ▼
┌──────────────────────┐   ┌──────────────────────┐
│ Deputy Data Protection│   │ Deputy Data Protection│
│    Officer (DDPO)     │   │    Officer (DDPO)     │
│     (Corporate)       │   │      (Schools)        │
└──────────────────────┘   └──────────────────────┘
          │                       │
          ▼                       ▼
┌──────────────────────┐   ┌──────────────────────┐
│ Senior Compliance     │   │ Senior Compliance     │
│  Officer x 2          │   │  Officer x 2          │
│  (Corporate)          │   │  (Schools)            │
└──────────────────────┘   └──────────────────────┘
          │                       │
          ▼                       ▼
┌──────────────────────┐   ┌──────────────────────┐
│ Compliance Officer x 2│   │ Compliance Officer x 1│
│  (Corporate)          │   │  (Schools)            │
└──────────────────────┘   └──────────────────────┘
```

RHONDDA CYNON TAF

Legal Drivers

- Ever changing data protection legal landscape
  - DPA1998
  - EU GDPR & DPA2018 (25th May 2018)
  - UK GDPR & DPA2018 (1st January 2021)

- Greater obligations on organisations with enhanced mandatory requirements

- Regulated by the Information Commissioners Office (ICO)
  - Monetary penalty notices – maximum fine of £17.5 million or 4x of annual global turnover
  - Enforcement notice – formal direction from the ICO to put things right or stop processing – 28 days
  - Assessment notice – ICO intention to carry out an audit
  - New Information Commissioner (5 year term)

- Local Government and Elections (Wales) Act 2021

RHONDDA CYNON TAF

ICO 'GDPR Accountability Framework'

Accountability is one of the key principles of data protection law – it makes us responsible for complying with legislation and requires us to demonstrate compliance.

The ICO 'GDPR Accountability Framework' is an opportunity for us to assess our organisational accountability.

10 key categories for accountability;

1) Leadership and oversight (governance)
2) Policies & procedures
3) Training & awareness
4) Individuals' rights
5) Transparency
6) Records of processing activities
7) Contracts and data sharing
8) Privacy risk assessments
9) Security
10) Breach/incident response

RHONDDA CYNON TAF

How we comply: Leadership & Oversight

- Regulated by the ICO

- Members
  - Scrutiny of governance arrangements at committees
  - Approval of policies

- Senior Leadership Team

- Senior Information Risk Owner
  - Board Member - SLT

- Information Management Board
  - Highlight report (breaches, SAR's, progress of key actions)

- Designated Data Protection Officer (statutory post)
  - Direct reporting line to SIRO

- ICT & Digital Service – Annual Service Self Evaluation

- ICT & Digital Service - Service Delivery Plan
  - Key Information Management actions
  - Monitored and reported quarterly to Performance Management

- Strategic Risk Register

RHONDDA CYNON TAF

How we comply: Policies & Procedures

- Comprehensive policy framework in place covering;
  - Data protection
  - Information security

- Operational procedures and guidance

- Policies and procedures provide staff with clear direction in relation to their roles and responsibilities for managing personal data and security

- Links to wider HR policies (e.g. disciplinary)

- Easily accessible on Inform and RCT Source

- Key points are reflected in the training we provide

RHONDDA CYNON TAF

How we comply: Data Protection Impact Assessments

A DPIA is a key risk management tool – it's a process that helps identity and minimise privacy risks.

Mandatory requirement to conduct a DPIA for processing that is likely to result in high risk – processing special category (sensitive) or criminal data, large scale processing, new technologies (invasive – monitoring, profiling, data matching etc.)

- DPIA framework developed
- DPIA Policy and supporting procedures drafted
- DPIA pre-screening arrangements in place
- DPIA's being conducted for high risk processing
- Escalation process in place for high risk processing that can not be mitigated (DPO > SIRO/IM Board > ICO)

RHONDDA CYNON TAF

How we comply: Information Rights

Information rights gives individuals greater control over their personal data.

We must make people aware of their information rights and how they can exercise them.

We must comply with information rights request within a specified time period.

- We inform individuals of their information rights
  - Website
  - Forms and applications

- Comprehensive guidance / procedures in place for staff;
  - Know how to recognise a request
  - Know how to respond to a request

- All subject access requests are recorded centrally by the Information Management team

- Subject access request training for key services
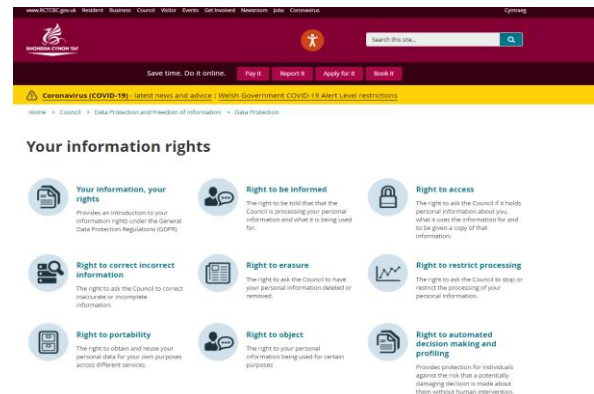
How we comply: Information Rights

2020-2021

157 requests received

104 requests validated

78% requests responded to within statutory timeframe

Service split:

Community & Children Services	66%
Chief Executive	8%
Prosperity, Development & Frontline	6%
Education & Inclusion	14%
Cross Cutting	6%

2021-2022 (April-Dec2021)

204 requests received

138 requests validated

83% requests responded to within statutory timeframe

Service split:

Community & Children Services	69%
Chief Executive	14%
Prosperity, Development & Frontline	1%
Education & Inclusion	7%
Cross Cutting	9%

RHONDDA CYNON TAF

How we comply: Transparency

The law requires that we are open, honest and transparent with individuals about the way we use their personal data

- General privacy notice published on the Council's website
- Over 90 service privacy notices published on the Council's website
- Data capture forms reviewed and updated signposting to notices
- Data protection logo that features on our website, letter heads etc.
- Elected Member privacy notice developed and published against each Members profile page (role as Ward Cllr)
- Approx. 20 privacy notice templates developed for use by Schools

DIOGELU DATA PROTECTION

MAE EICH DATA O BWYS
Am ragor o wybodaeth am sut rydyn ni'n defnyddio'ch data, ewch i www.rctcbc.gov.uk/diogeludata

YOUR DATA MATTERS
For more information about how we use your data visit www.rctcbc.gov.uk/dataprotection

How we comply: Record of processing activities

The law requires that we maintain a record of our processing activities. These records must be made available to the ICO upon request.

- Extensive data mapping exercise undertaken upon GDPR to baseline our processing activities;
    – What data we hold
    – Why we hold it
    – Where we hold it and in what format
    – Who we share it with and why
    – How long we keep it for

- Data Protection Register established
    – Formally records our data processing activities
    – Identifies the lawful basis for processing (for each activity)

- Live document – constantly being reviewed and updated

RHONDDA CYNON TAF

How we comply: Breach (incident) response

The law requires;

- **that we have robust breach detection, investigation and internal reporting procedures in place.**
- **that we report certain serious breaches to the ICO within 72 hour of becoming aware and we inform data subject of a high risk breach that may adversely affect their risks and freedoms.**
- **keep a record of any breach (regardless of severity)**

- Well established incident response procedures in place.
- Specific procedures in place for dealing with cyber incidents and a dedicated Incident Response Team
- All staff have a personal responsibility to report breaches (actual/suspected)
- Requirement to report covered in staff training.
- All breaches are recorded, thoroughly investigated and documented.
- Escalation process in place for serious personal data breaches (DPO to SIRO)
- Notification to ICO for serious breaches
- Notification to data subject for high risk

RHONDDA CYNON TAF

How we comply: Breach (incident) response

2020-2021

- 127 incident/events reported and investigated.

- 14% classed as events

- 86% classed as incidents

- 9 breaches reported to ICO
  – 8 – no further action
  – 1 – awaiting outcome

2021-2022 (April-Dec2021)

- 96 incident/events reported and investigated.

- 8% classed as events

- 92% classed as incident

- 7 breaches reported to ICO
  – 5 – no further action
  – 2 – awaiting outcome

RHONDDA CYNON TAF

How we comply: Training & Awareness

- Mandatory e-learning training

- Face-to-face training
  - Bespoke training (e.g. Team setting)
  - Elected Members
  - Head Teachers
  - School Governors
  - Data Protection Leads (Schools)

- Awareness
  - Bulletins - cyber security
  - Corporate Induction
  - Managers Briefings
  - Senior Management Team meetings

Key Priorities for 2022-2023

- Deliver key services under our Service Level Agreements

- Deploy new mandatory data protection e-learning training to staff and Members

- Develop e-learning data protection training module for all School staff.

- Review key Council and Schools information security policies to ensure they remain complaint with legislation and government guidance.

- Support the governance arrangements for Phase 2 of the South East Wales Corporate Joint Committee

- Support the delivery of the Council's Digital Strategy 2022-2026 (currently in draft)

RHONDDA CYNON TAF

Questions

?

RHONDDA CYNON TAF