

Data Protection Risk Management

Martin Aust

Head of Intelligence

DPA – Key requirements

- Personal data processed fairly and lawfully
- Should be adequate, relevant & not excessive
- Shall be accurate and kept up to date
- Not kept longer than necessary
- Appropriate technical and organisational measures in place

Our organisational approach....

- Prevention better than cure
- Focus on preventing harm foremost
- DP as enabler, not a barrier
- Equip staff with knowledge and tools
- Built on management & personal responsibility
- Transparency and openness
- Continuous improvement – learn lessons

Organisational framework - features

- Included on the Corporate Risk Register
- Audit oversight – Committee & Internal Audit
- Visibility – weekly DP report to management
- Central DP team integrated with FOI/SAR/RM
- Advice and guidance on DP compliance
- Privacy by design methodology employed
- Robust and extensive policy framework...

Policy Framework

Data Protection Policy



Metadata

Type: Policy
Classification: Unclassified
Author: Martin Aust
Issuing body: Corporate Services
Authoriser: Predates Compass
Team: Data Protection Team
Date created: 01 Dec 1999
Version date: 08 Dec 2014
SO:

Contents

Summary
Document information
Introduction
Objectives
Roles and Responsibilities
Policy
See whole policy
Print policy

Summary

This policy sets out the requirements for the protection of personal data under the Data Protection Act 1998.

Corporate Information Security Policy



Corporate Information Security Policy

Type: Policy
Classification: Unclassified
Author: ICT Policy & Procedure
Issuing body: Resources and Performance
Authoriser: John Alleyne
Team: ICT Policy & Procedure
Date created: 15 Mar 2010
Version date: 15 Mar 2010
Issue: 2.1
SO:

Contents

Introduction
Scope
Monitoring & Breach
Roles & Responsibilities
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Compliance
Glossary
See whole policy
Print policy

Summary

The Corporate Information Security Policy assigns responsibilities to individual users of information (and establishes minimum confidentiality, integrity, and availability of all information) to affect Hertfordshire County Council legal requirements.

Code of Conduct



Code of Conduct

Metadata

Type: Policy
Classification: Unclassified
Author: Melanie West
Issuing body: ...
Authoriser: Predates Compass
Team: Strategy and Policy
Date created: 08 Oct 2010
Version date: 01 Aug 2013
Issue: 2
SO:

Contents

Key Points
Introduction
Scope
Standards
Disclosure of Information and
Political Neutrality
Relationships
Contracting and Tendering
Appointment and Employment
Outside Commitments and
Equality and Diversity
Financial Resources
Gifts, Hospitality and Sponsorship
See whole policy
Print policy

Summary

Legal Framework: The Constitution under which the County Council operates is the Constitution which is available at [www.hertfordshire.gov.uk](#)

Corporate Information Security Policy



Corporate Information Security Policy

Metadata

Type: Policy
Classification: Unclassified
Author: ICT Policy & Procedure
Issuing body: Resources and Performance
Authoriser: John Alleyne
Team: ICT Policy & Procedure
Date created: 15 Mar 2010
Version date: 15 Mar 2010
Issue: 2.1
SO:

Contents

Introduction
Scope
Monitoring & Breach
Roles & Responsibilities
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Corporate Rules
Compliance
Glossary
See whole policy
Print policy

Summary

The Corporate Information Security Policy assigns responsibilities to individual users of information (and establishes minimum confidentiality, integrity, and availability of all information) to affect Hertfordshire County Council legal requirements.

Records Management Policy

RECORDS MANAGEMENT POLICY

Resources and Performance

Release:
Policy version:
Owner:
Date:
Document version:
Author:

Published
3
Hertfordshire County Council
29th January 2015

Summary

This policy sets out Hertfordshire County Council's approach to Records Management, in line with the requirements set out in the Lord Chancellor's Code of practice on the management of records issued under section 46 of the Freedom of Information Act 2000 ("the Section 46 Code") and associated legislation and regulations. The policy covers all of the council's records, irrespective of their format or the technology / method used to create and store them. It details the processes and procedures which staff must follow to ensure they comply with statutory and operational requirements. Advice and guidance on Records Management, and compliance with this policy, is available from the Information Governance Unit's Records Management Helpline.

So what do we do? – Technical (1)

- Industry approved security measures (firewalls, email filtering software, desktop AV)
- Network security standards, including penetration testing
- ICT service provider compliance with security standards
- Encryption – laptops & other portable media

So what do we do? – Technical (2)

- HertsFX allows secure transfer of documents between HCC and any invited partner
- GCSX/N3 - secure email exchange with other key partners – Police, NHS
- Smart Worker – electronic access/working
- Technical procedures for avoiding unintended disclosure of personal data
- 2016 Printer roll-out – reduce paper left visible and unintended data added to mailing

So what do we do? – Training

- Training – vital link between policy & practice
- DP iLearn module mandatory for new staff
- Not “spray and pray”
- Targeted training for staff handling sensitive personal data – e.g. Social care, HR, Legal
- Supplemented by role based training
- Awareness raising – reinforce best practice

So what do we do? – Procedural (1)

- Apply learning – “sum of marginal gains”
- Peer checking for sensitive paper/post or email address
- Make sure undelivered post returns to HCC – return address; mark envelope “personal & confidential”
- Separation of secure high value IT kit targeted by thieves and paper-based information

So what do we do? – Procedural (2)

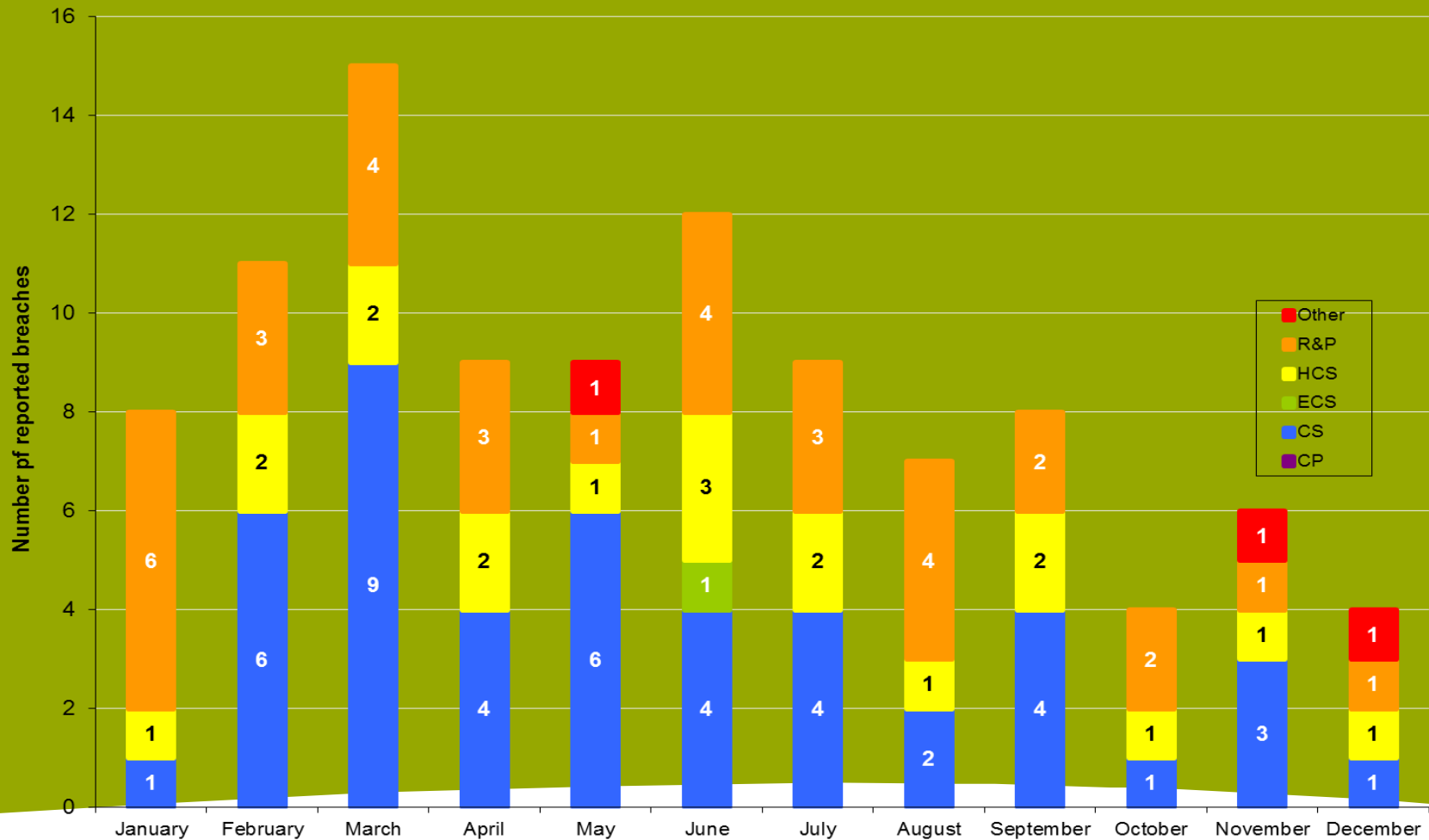
- Data sharing agreements/toolkit in place
- For use in partnership settings – care focus but applied in other settings
- Integrated with Privacy Impact Assessment which identifies risks
- Caldicott Guardian in place and trained for social care data sharing
- Governance through data sharing workstream in ICT Strategy

So whatwhat is our record?

- Potential breaches per year – 40,000,000+
- Subject to ICO fine - £500,000
- No potential breaches met threshold for reporting to ICO since 2010
- No potential breaches met threshold for reporting to NHS
- IG Level 2 toolkit NHS accreditation achieved
- Significant decline in number of breaches.....

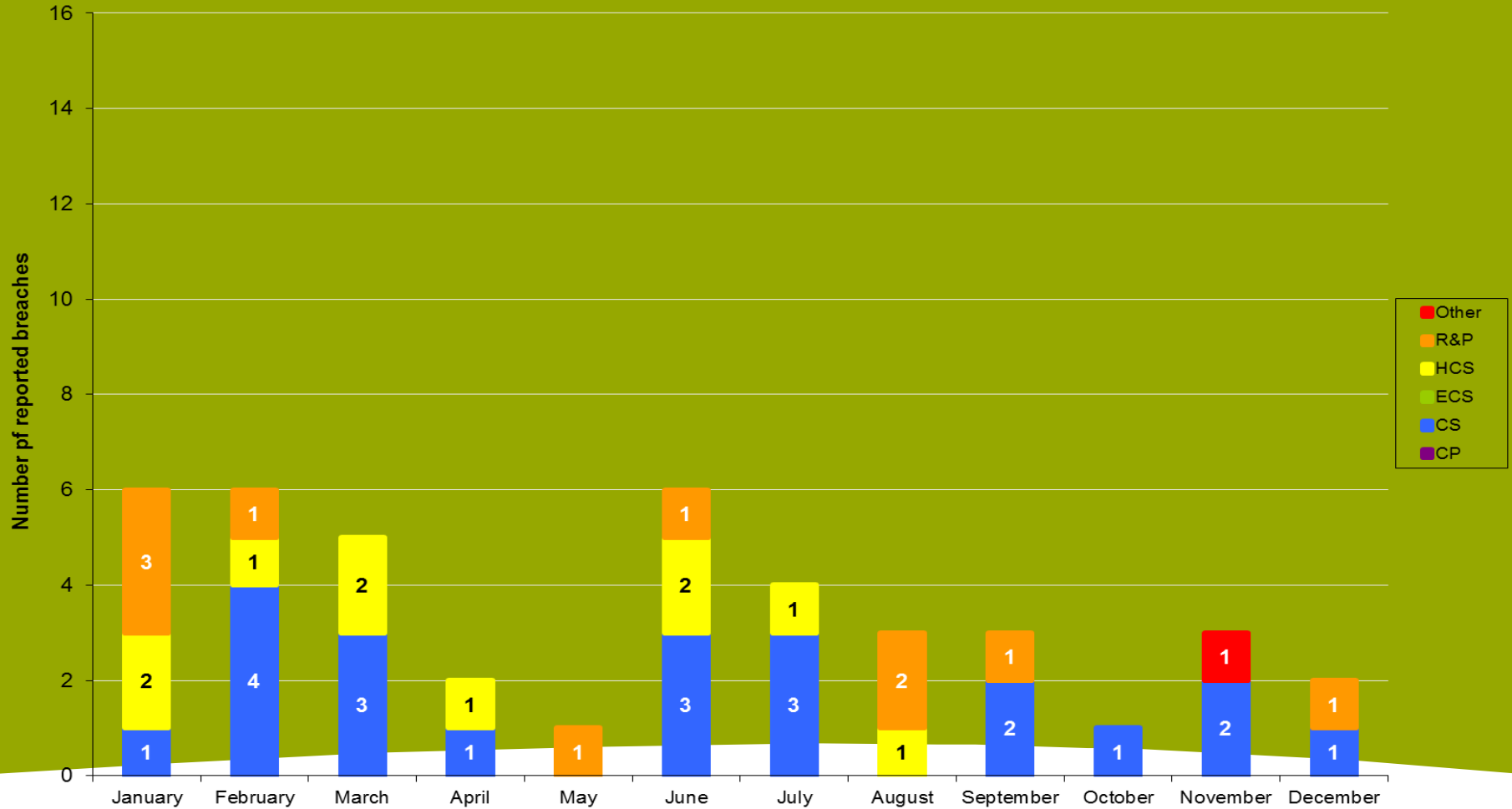
Data Protection Breaches 2014

DP breaches reported to the DPT 2014



Data Protection Breaches 2015

DP breaches reported to the DPT 2015



Looking forward - EU General Data Protection Regulation 2018 (GDPR)

- European Directive which formed the basis of 1998 DPA not now fit for purpose.....
 - New forms of personal data
 - Internet and technical facilities for sharing/publishing personal data
 - Commercial exploitation of personal data Facebook; Fitbit; donor data passed between voluntary organisations.
- All member states will adopt this and measures will need to be in place for implementation in 2018

EU GDPR 2018 - implications

- Maximum of €10m for some breaches - Data loss feature here
- Maximum of €20m for other breaches, e.g. unlawful processing, right to be forgotten
- Mandatory breach reporting to regulator within 72 hours *unless the breach is unlikely to result in a risk for the rights and freedoms of individuals*
- Responsibility to inform Data Subject where high risk to the rights and freedoms of individual
- Aligns with current approach – but impact greater

thank you

www.hertsdirect.org

