

Public Document Pack

NOTTINGHAM CITY COUNCIL

AUDIT COMMITTEE

MINUTES of the meeting held at Ground Floor Committee Room - Loxley House, Station Street, Nottingham, NG2 3NG on 24 November 2017 from 10.31 am - 12.18 pm

Membership

Present

Councillor Sarah Piper (Chair)
Councillor Leslie Ayoola
Councillor Rosemary Healy
Councillor Anne Peach
Councillor Andrew Rule
Councillor Adele Williams
Councillor Malcolm Wood (Vice Chair)
Councillor Steve Young

Absent

Councillor John Hartshorne

Colleagues, partners and others in attendance:

| | | |
|----------------|---|---|
| Tony Crawley | - | KPMG |
| Elaine Fox | - | Policy Development Officer |
| Jane O'Leary | - | Insurance and Risk Manager |
| Kate Morris | - | Governance Officer |
| Naomi Matthews | - | Data Protection Team Leader - Via Skype for minute 33a only |
| Sue Risdall | - | Finance Analyst |
| Shail Shah | - | Head of Audit and Risk |
| John Slater | - | Group Auditor |
| Thomas Straw | - | Senior Accountant Capital Programme |
| Thomas Tandy | - | KPMG |
| Amanda Wright | - | Customer Experience Lead |

28 APOLOGIES

Councillor John Hartshorne – personal

29 DECLARATIONS OF INTEREST

None.

30 MINUTES

The minutes of the meeting held on 22 September 2017 were agreed subject to the following change:

Minute 24 point (i) complete set of accounts was required by 30 June 2017, not 12 June 2017.

31 REVIEW OF ACCOUNTING POLICIES 2017/2018

Susan Risdall, Finance Team Leader for Technical Accounting introduced a report on the Review of Accounting Policies 2017/18. She informed the committee that there were no major changes to the policies and that they would be passed to the external auditors for review. There was a short discussion on the changes as detailed in the appendix to the report, published as part of the agenda.

RESOLVED to:

- (1) Review and agree the Statement of Accounting Policies, as set out in appendix one of the report published as part of the agenda, for inclusion in the 2017/18 annual Accounts; and**
- (2) Review and agree the proposals where International Financial Reporting Standards allow a degree of choice.**

32 OMBUDSMAN ANNUAL LETTER

Amanda Wright, Customer Experience Lead, introduced a report on the Ombudsman Annual Letter containing a reflection of the complaints received and decisions made on complaints about Nottingham City Council by the Local Government Ombudsman from April 2016 to March 2017. The following points were highlighted:

- (a) In June 2016 the way customer complaints were handled by the Council was reviewed and altered to focus more on the quality of the response to complaints at the first stage of the process to ensure a full and thorough response is given;**
- (b) the rate that the Ombudsman upheld complaints was down from 48% in 2015-16 to 35% in 2016-17. This is below the national rate of 54% and below the regional rate of 44%;**
- (c) the complaints received reflect national trends with Adult Care, Benefits and Tax and Education and Children's Services being the main subjects of complaint.**

RESOLVED to thank Amanda Wright for her attendance and to note the contents of her report.

33 CORPORATE RISK

a PRESENTATION ON GDPR (Agenda Item 6a)

Naomi Matthews, Data Protection Team Leader and Senior Solicitor gave a presentation on the General Data Protection Regulations. The comprehensive presentation is appended to these minutes.

RESOLVED to thank Naomi Matthews for her presentation on the General Data Protection Regulations and to note its content;

b PRESENTATION ON STP (Agenda Item 6b)

Colin Monkton, Director of Strategy and Policy and Helen Jones Director of Adult Social Care, gave a presentation on the Sustainability and Transformation Partnership (STP). They highlighted the following key points:

- (a) The key objectives of the STP include benefiting citizens by providing less fragmented care, providing a population focused service and reducing variation in levels of referral and practice standards;
- (b) the Greater Nottingham Health Care Partnership, which Nottingham City Council is included in, is 1 of 2 delivery groups within the STP;
- (c) Nottingham City Clinical Commissioning Group (CCG) has now merged with 3 smaller CCG to cover the whole of the Greater Nottingham area;
- (d) Greater Nottingham has been named accelerator for the Accountable Care System which is an integrated system of providers with joint responsibility to deliver outcomes at a population level;
- (e) focus on aligned targets and engagement in joint commissioning with the CCG are factors that will help the new system, which will help the Greater Nottingham area operate in the most efficient way whilst improving access;
- (f) there is currently a review of Adult Social care practice taking place with an aim to identifying any savings potential and will take a view on clinical variance and differing practices across the partnership.

The Committee made a number of comments and asked some questions. The following information was highlighted:

- (g) There is a more focused emphasis on outcomes for individuals and giving them the ability to live the best life that they can through re-enablement and encouraging independence;
- (h) the Chair of the Health Scrutiny Committee confirmed that the Health Scrutiny Committee receives regular updates on the progress of the STP. It is looking closely at the governance, partnerships and commissioning arrangements of the partnership. Along with the formal scrutiny from the Committee there are also informal meetings with Health Scrutiny Committee members in between committee dates;

RESOLVED to thank Colin Monckton and Helen Jones for their attendance and to note the content of their presentation on the Sustainability and transformation Partnership.

c RISK REGISTER (Agenda Item 6c)

Jane O'Leary, Insurance and Risk Manager, presented the Corporate Risk Register Update for Q2 to the Committee. She advised the Committee that the risk register

had been approved by the Corporate Leadership Team on 15 November 2017. One new risk had been added, SR14, relating to trading companies governance.

RESLOVED to:

- (1) note the risk identified on the Q2 Corporate Risk Register;**
- (2) select SR4 relating to potential changes in taxation for consideration at a future meeting; and**
- (3) select SR8 relating to IT security for consideration at a future meeting.**

34 TREASURY MANAGEMENT 2017/18 HALF YEARLY UPDATE

This item was withdrawn from the agenda and will be brought to the February Committee Meeting.

35 INTERNAL AUDIT QUARTERLY REPORT 2017/18 (Q1 & Q2)

Shail Shah, Head of Audit and Risk introduced the Internal Audit Quarterly report which outlined the work of the Internal Audit service for the first and second quarter of 2017/18. He highlighted the following points to the Committee:

- (a) All local Performance Indicators are being met and the Audit Service is on target to meet the Audit Plan 2017/18;
- (b) work continues around company governance review as discussed at the last meeting, including the requirements of the UK Corporate Governance Code and best practice on governance of local authority controlled companies approach the subject. It is expected that a project update or full report will be presented to the February meeting.

Following questions from Committee members the following further information was given:

- (c) The schools mentioned in the report are Local Authority Schools, the Audit Service does complete commercial Audit work for 3 academies and a number of out of county schools but these are not reflected in the report.
- (d) full internal audit reports on items where there is limited assurance will be circulated to all Committee members for review. If members feel it necessary to look at any report then it will be brought to a future committee meeting;

RESOLVED to note the performance of Internal Audit during quarter 1 and quarter 2 of 2017/18

36 COUNTER FRAUD STRATEGY

Shail Shah, Head of Audit and Risk introduced the report on the Counter Fraud Strategy which sought endorsement from the Committee. The Committee took the report as read and gave its endorsement.

RESOLVED to:

- (1) Endorse the City Council's updated Counter Fraud Strategy (CFS) set out in appendix 1 of the report published as part of the agenda; and**
- (2) Endorse the Counter Fraud Strategy for Schools (SCFS) set out in appendix 2 of the report published as part of the agenda.**

37 AUDIT COMMITTEE TERMS OF REFERENCE AND ANNUAL WORK PROGRAMME

Shail Shah, Head of Audit and Risk introduced the report on the Audit Committee Terms of Reference and Annual Work Programme.

RESOLVED to:

- (1) Note the role and functions of the Audit Committee including the additional elements prescribed by the Public Sector Internal Audit Standards (PSIAS) and the benefits arising from its existence; and**
- (2) Endorse the outline work programme set out in appendix 1 of the report published as part of the agenda, including the Assurance Plan and the Terms of Reference at Appendices 2 and 3.**

38 PARTNERSHIP GOVERNANCE ANNUAL HEALTH CHECKS OF NOTTINGHAM CITY COUNCIL'S SIGNIFICANT PARTNERSHIPS

Elaine Fox, Policy Officer, introduced the report in the Partnership Governance Annual Health Checks of Nottingham City Council's Significant Partnerships. She highlighted the following points:

- (a) There are currently 11 partners on the register and the majority of partnerships scored either good or excellent in all areas;
- (b) the Midlands Engine was added to the Register of Significant Partnerships in 2017;
- (c) the N2 Skills and Employment Board scored itself 2 for Partnership risk management due to funding coming to an end in March 2018. A score of 3 would be more appropriate as funding has not been agreed for six months time and this leave little opportunity for planning;
- (d) D2N2 Local Enterprise Partnership (LEP) scored itself 3 for Partnership Risk Management. Risk assessments are in place for individual projects but there

is currently no overall risk register. This is currently being addressed as part of the Local Assurance Framework;

- (e) D2N2 also have to deal with conflicts of interest which increases the risk for Partnership Management. This is an issue for all LEPs. No LEP partner is responsible for making decisions in isolation and it is expected that, following the review of the Local Assurance Framework, the score will improve in 2018;
- (f) Safeguarding Children's Board scored itself 3 for finance due to pressures on the proposed budget for 2017/18. However the partnership confirmed that the budget is sufficient to deliver its business plan and so a score of 2 is more suitable;
- (g) the Midlands Engine scored itself 3 for Equalities. As the partnership was included on the register this year they will be verified in 2018 and an improvement in the score should be seen at that point;
- (h) all partners have confirmed that they are engaged with the Data Protection Team and will undertake any action necessary to ensure they are prepared for the introduction of General Data Protection Regulation (GDPR). A question will be added to the Health Check survey in 2018 asking partners to rate compliance with GDPR;

Following questions from the Committee the following information was given:

- (i) The Green Partnership has no score for Finance as the partnership does not receive funding. The partnership has been verified for the last 2 years and not verifying it in 2018 will give the new governance, structure and policies time to take effect and improve scores.

RESOLVED to:

- (1) to note the key findings from the Partnership Governance Health Checks and Register of Significant Partnerships; and**
- (2) to note the findings and recommendations following verification of governance documentation of four of the partnerships.**

Data Protection Update: Preparing for General Data Protection Regulation GDPR

Page 7



Minute Item 33a

Naomi Matthews



Nottingham
City Council

Aims of the session



- Consider what changes the new General Data Protection Regulation will bring about
- What preparations does Nottingham City Council need to make for next May
- Look at some recent data breaches and their relevance to NCC

Page 8



Nottingham
City Council

The General Data Protection Regulation GDPR

- Comes into force on the 25 May 2018
- Data Protection Act 1998 will be repealed
- Data Protection Bill currently in House of Lords- this supplements the GDPR.



Increased enforcement powers

- New fines will be imposed on a two tier basis
- For contraventions such as record keeping and data processor contracts, failure to notify breaches within 72 hours a fine of 2% of turnover or 10 million Euros
- For contraventions of data protection principles, data subject rights the fine will be up to 4% of annual turnover or 20 million Euros

Page 10



Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now



1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3
Page 1

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5

Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7

Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11

Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

GDPR Awareness campaign

1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Page 12

- 12 steps campaign on plasma screen
- Communications plan
- GDPR Action plan
- IMAB project plan for GDPR
- Working group- meeting on monthly basis to try and include all key stake holders



From **May 2018** the Data Protection Act 1998 will be replaced by the **General Data Protection Regulation**



Step 1: Awareness

Page 13

Decision makers and key people must be aware of the changes and appreciate the impact this is likely to have



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



**Nottingham
City Council**

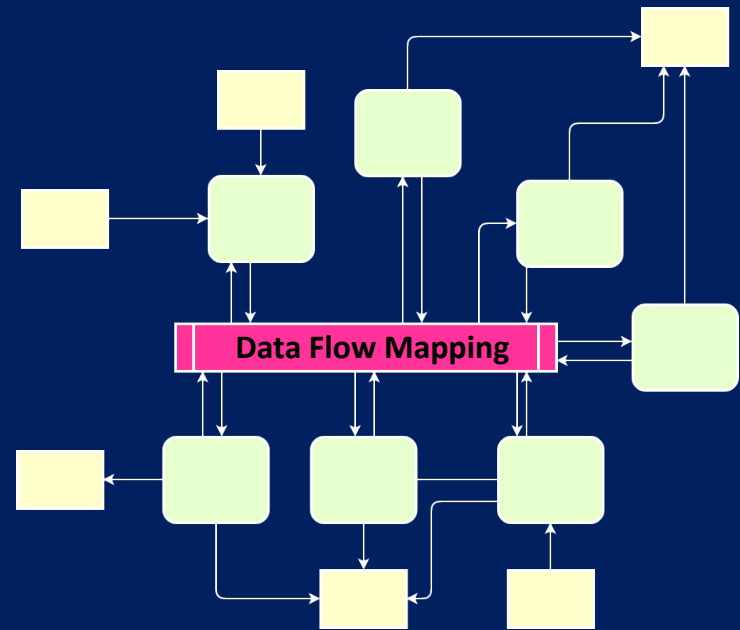
12 Steps of GDPR

Step 2: Information you hold

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

Every team will need to document:

- **what** personal data is held
- **where** it came from
- **who** it is shared with
- **how** it is shared (risk assessments).



 **Data Protection Team: ext. 63855**
 **data.protection@nottinghamcity.gov.uk**



Safe, clean, ambitious, proud



**Nottingham
City Council**

12 Steps of GDPR

Step 4: Individual's Rights

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

Do your procedures cover all the rights individuals have?

Page 15

- How personal data is deleted
- How it is provided
- How it is used



 Data Protection Team: ext. 63855
 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

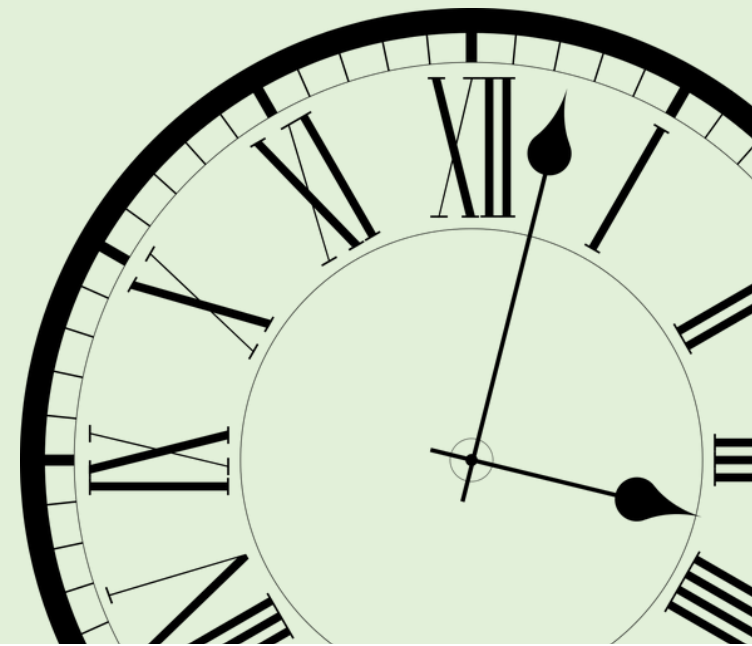
Step 5: Personal information Request (PIR)

Citizens can request their personal information to be provided:

Page 16

- Free of charge
- Within a month

 **Data Protection Team: ext. 63855**
 **data.protection@nottinghamcity.gov.uk**



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

Step 6: Lawful basis for processing personal data

By May 2018 you must:

- Identify the lawful basis for your processing activity
- Document it
- Update your privacy notice to explain it.

Page 17



 Data Protection Team: ext. 63855

 data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 7: Consent

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**

You must review how you **seek, record and manage** consent. Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk



Safe, clean, ambitious, proud



Nottingham
City Council

12 Steps of GDPR

Step 8: Children

Begin to think whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any on-line website for children

Page 19



 Data Protection Team: ext. 63855

 Data.protection@nottinghamcity.gov.uk

From **May 2018** the Data Protection Act 1998 will be replaced by the EU's **General Data Protection Regulation**



Safe, clean, ambitious, proud



Nottingham
City Council

Record keeping and audit of information- Data flow mapping

- Under A 30 the organisation must maintain a record of processing operations under its responsibility
- The record should be seen as a tool to allow an overview of all the personal data processing activities an organisation is carrying out
- Prerequisite for compliance
- Effective accountability measure for the Council

Page 20



GDPR – Information Audit

2

Information you hold

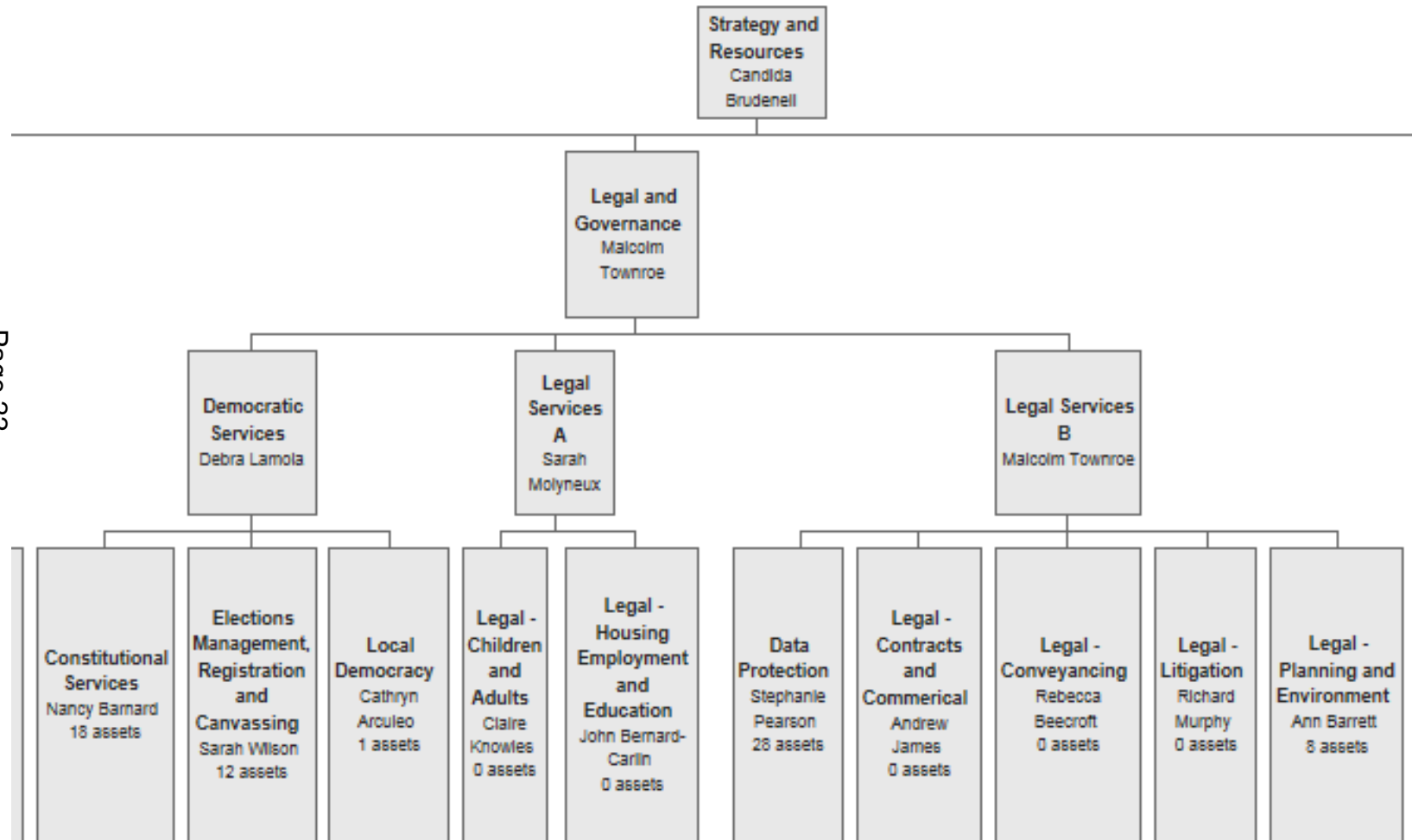
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

- Spreadsheet to carry out Data flow mapping is currently being developed by the DP team/ RM team
- The template will need to be populated by each department in the council – a huge task!
- The Information Asset Register should hold this information, the legal basis of processing and any linked privacy notice, PIA and ISA = records of processing

Organisational charts

Strategy and Resources

ONLY Business Functions which have been assigned a Service Area can be included in this chart.

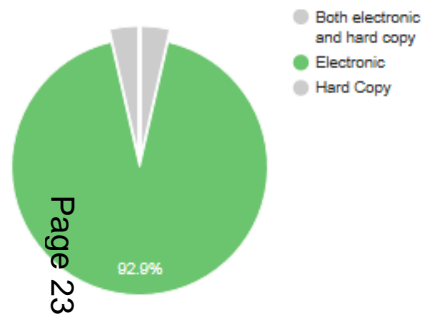


Data Protection

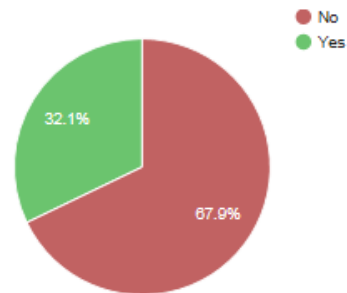
Filtered by Business Function - 28 results.

[Back](#) [Export to Excel...](#)

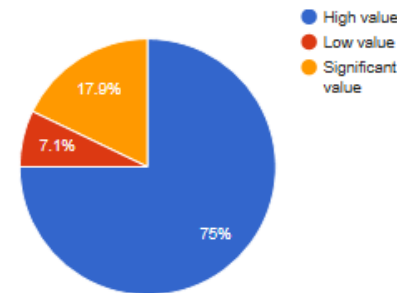
Resource format



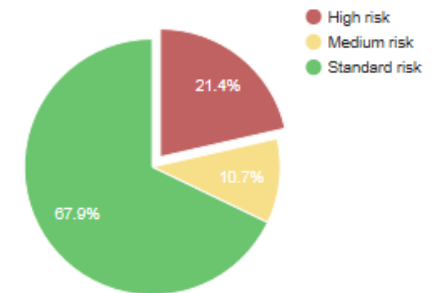
Personal information



Relative value



Risk factor



| ID | Name | Description | IA Manager | PI? | Retention period | Business function | Combined risk | |
|-----|---|---|-------------------|-----|------------------|---|------------------------------|-------------------------|
| 157 | Body Worn Video (BWV) surveillance system guidance | Community Protection Officer's Guidance notes on Body Worn Video (BWV) surveilla... | Stephanie Pearson | No | 0 years ... | Data Protection Strategy and Resources » Legal and Governance » Legal Services B | Business: 3 Individual: 0 | Details |
| 158 | Data Protection - The Act, Policy and Practice guidance | Summary of how the Data Protection Act affects colleagues, and what to do if a d... | Stephanie Pearson | No | 0 years ... | Data Protection Strategy and Resources » Legal and Governance » Legal Services B | Business: 5 Individual: 0 | Details |
| 161 | Personal data requests handling guidance for frontline | Guidance on how to handle requests for personal data. This | Stephanie Pearson | No | | Data Protection Strategy and Resources » | Business: 4 Individual: 1 | Details |

GDPR- Privacy Information

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Page 24

All consent forms throughout the Council have privacy notices that will need to be reviewed

- There is also a privacy notice on the main intranet that was agreed by Legal Counsel but will be out of date by next May

GDPR Individual rights

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

- Page 25
- Right to rectification
 - Right to erasure (right to be forgotten)
 - Right to restriction of processing
 - Right to data portability
 - Right to object



GDPR Subject Access Request

5

Subject access requests

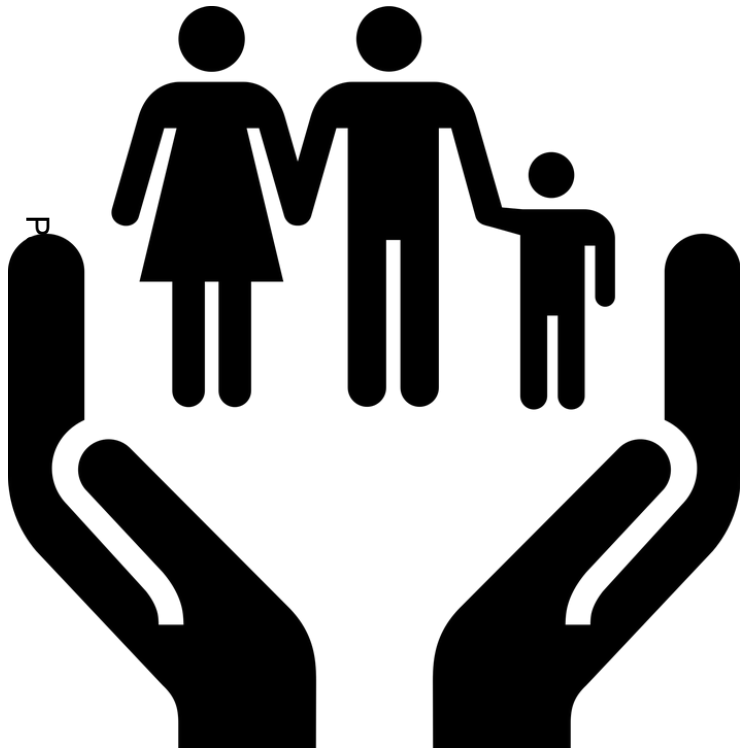
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Page 26

- Subject Access procedure is changing.
- No fee
- They will need to be provided with more information including extra rights, retention period, purposes of processing, how to lodge a complaint etc.
- Times have been reduced for compliance of standard SARs making compliance targets more difficult



Subjects rights under GDPR



- Right to access personal information- Personal information requests (PIR's)
- Once the information audit is completed DP team will be in a position to provide the personal information and the information required to be given by A 15



GDPR Purpose of processing

6

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

There are many reasons for processing data.

- Consent is one way.
- Others include: Contractual purpose, Legal obligation, statutory power. These gateways are changing for Local Authorities.
- New gateway – Public duty



GDPR Purpose of processing

6

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

Page 29

6 Principles (Article 5)

1. Personal data shall be:

- a) Fair, lawful and transparent
- b) Specific, explicit, legitimate purposes
- c) Adequate, relevant, necessary
- d) Accurate, where necessary up to date
- e) Retention
- f) Security



GDPR Purpose of processing

Page 30

Lawfulness of processing *(Article 6)*

1. One of the following

- a) Consent
- b) Performance of contract
- c) Legal obligation
- d) Vital interests
- e) Public interest/ exercise of Authority
- f) Legitimate interest (not for local Authorities and most schools)



GDPR Purpose of processing

Page 31

Special Data (*Article 9*)

2. a) Explicit consent
- b) Employment/ social security/ social protection obligations
- c) Vital interests
- d) Non-profit bodies
- e) Processing made public by data subject
- f) Legal claims
- g) Substantial public interest
- h) Health, social care, medicine
- i) Public interest for public health
- j) Archiving, statistics, historical research



GDPR Purpose of processing

Page 32

Adhere to
6 principles in
Article 5

Select gateway
from
Article 6

For **special
data**
select gateway
from
Article 9

= **Lawful
processing**



Nottingham
City Council

GDPR Consent

7

Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

Page 33

- Many consent forms will need reviewing
- Systems will need to identify whether consent is a reason for processing
- No pre ticked boxes
- Must opt in not opt out



Lawful basis of processing



- Where processing is based on consent must be explicit
- Page 34 However ICO draft guidance on consent notes that the main basis the local Authorities will use to process data is public task/ public interest
- This will be a big culture change for parts of the Council



GDPR Children's rights

8

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

Page 35

- We are still waiting for UK to verify what age children will be required to give consent
- Parts of the council may need to obtain both children and adults consent to process their children's data.
- More rights for children under the GDPR



GDPR Data Breaches

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.



Page 36

A situation or incident that results in, or has the potential to result in, a breach of one or more of the data protection principles.

- Data breaches will need to be notified to the ICO within 72 hours
- Not all breaches will need to be notified to the ICO

Greater Manchester Police

The following is an example of a data protection breach involving lost post.

Page 37



You are here → [News](#)

UKA correspondent

Friday 5 May 2017

[in Share](#)

[f Share](#)

[t Share](#)

ICO hits Manchester Police with £150,000 fine

Information commissioner sanctions force for losing unencrypted DVDs of victim interviews

The Information Commissioner's Office (ICO) has hit Greater Manchester Police (GMP) with a £150,000 fine for losing three DVDs containing footage of interviews with victims of violent or sexual crimes.



The force sent the unencrypted DVDs, which showed named victims talking openly, to the Serious Crime Analysis Section (SCAS) of the National Crime Agency in the post by recorded delivery but they were never received. The DVDs have never been found.

An investigation by the Information Commissioner's Office (ICO) found that the police force failed to keep highly sensitive personal information in its care secure and did not have appropriate measures in place to guard against accidental loss. This is a breach of data protection law.

Basildon Borough Council

The following is an example of a data protection breach involving information posted on a planning portal.

Page 39



Security

30

UK council fined £150k for publishing traveller family's personal data

Medical details exposed in online planning application

By [Kat Hall](#) 31 May 2017 at 15:08

SHARE ▼

An Essex council has been fined £150,000 for publishing highly sensitive personal data, including medical information, of a traveller family via online planning documents.

The Information Commissioner's Office (ICO) slapped Basildon Borough Council for publishing the information in planning application documents, which it made publicly available online for nearly two months.

The council published a full statement containing sensitive personal data relating to a static traveller family who had been living on the site for many years. It referred to the family's disability requirements, including mental health issues, the names of all the family members, their ages and the location of their home.

The ICO's investigation found that on 16 July, 2015, the council received a written statement in support of a householder's planning application for proposed works in a green-belt area. The information was only removed on 4 September when the concerns came to light.



Case Study – Stoke on Trent City Council

The following is a physical loss of a Child's personal information

Page 41



ICO hits Stoke-on-Trent City Council with £120,000 fine



Jennifer Scott
TechTarget
26 Oct 2012 11:26



Stoke City Council has breached the Data Protection Act, for the second time in two years, after details of a child protection legal case were emailed to the wrong person.

Stoke-on-Trent City Council has been fined £120,000 by the Information Commissioner's Office (ICO) for breaching the Data Protection Act.

A solicitor that worked within the organisation was found to have sent 11 emails containing information about a child protection law suit to the wrong person, which the ICO considered a "serious breach"



Page 42

GDPR- Privacy by design

10

Data Protection by Design and Data Protection Impact Assessments

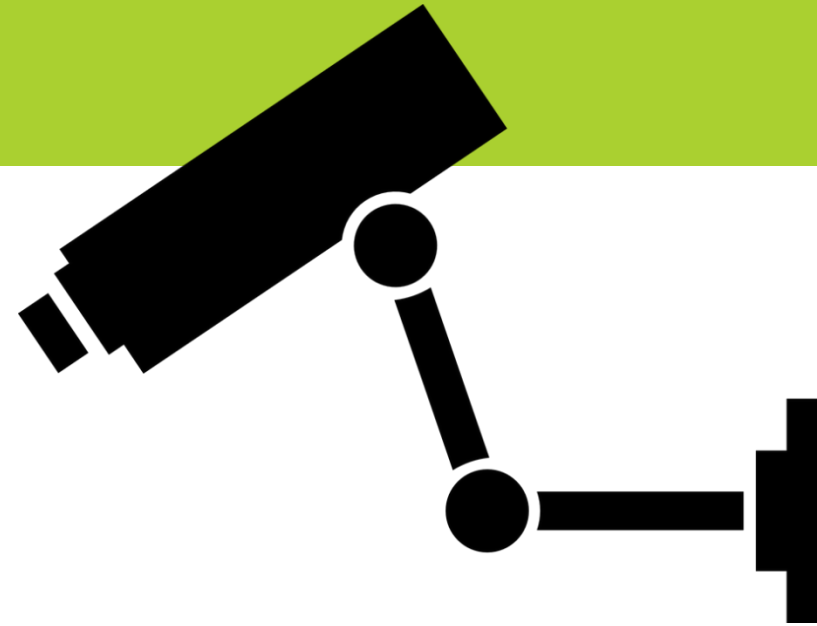
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

Page 43

- Where a new type of processing/project takes place using new technologies where there is a high risk to privacy a privacy impact assessment **must** be carried out
- Assessment must look at necessity and proportionality
- Needs to be embedded in process



Data Protection Impact Assessments- DPIA (formerly PIA)



- CCTV
- Body worn Cameras
- Camera in cars/Outside cars
- New APPs that collect lots of sensitive data
- New systems such as liquid logic, Case management systems

Page 44



GDPR Data Protection Officers

11

Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.



Page 45

- Under Article 37 a Data Protection Officer must be appointed where processing is carried out by a public authority. The Data protection officer has to report to the highest management
- Must have expert knowledge of data protection
- Cannot undertake tasks that could create a conflict of interest



GDPR International

12

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Page 46

- Any information held on cloud systems outside the EU
- Contracts with companies in Non EU countries
- Correspondence with citizens / relatives abroad

